sifma

Internal Auditors Society

Internal Audit Guidelines
Fraud Risk in Broker-Dealers

March 2013

The Audit Guidelines (the "guidelines") are intended to provide members of the Internal Auditors Society ("IAS"), a society of the Securities Industry and Financial Markets Association ("SIFMA"), with information for the purpose of developing or improving their approach towards auditing certain functions or products typically conducted by a registered broker-dealer. These guidelines do not represent a comprehensive list of all work steps or procedures that can be followed during the course of an audit and do not purport to be the official position or approach of any one group or organization, including SIFMA, or any of its affiliates or societies. Neither SIFMA, nor any of its societies or affiliates, assumes any liability for errors or omissions resulting from the execution of any work steps within these guidelines or any other procedures derived from the reader's interpretation of such guidelines. In using these guidelines, member firms should consider the nature and context of their business and related risks to their organization and tailor the work steps accordingly. Internal auditors should always utilize professional judgment in determining appropriate work steps when executing an audit. Nothing in these guidelines is intended to be legal, accounting, or other professional advice.

sifma

Internal Auditors Society

TABLE OF CONTENTS

This is not an exhaustive list of fraud risks and related audit procedures that audit practitioners need to follow during an audit of controls over the risk of fraud in broker-dealers. Further, not all procedures will be applicable to your organization. Audit practitioners must consider factors such as the firm's risk and exposure with respect to size, business lines, customer base and geographic location in determining the appropriate procedures. Further, the audit practitioner should be familiar with current laws, regulations, and guidance materials.

sifma

Internal Auditors Society

I. INTRODUCTION AND BACKGROUND

A. Overview

The Audit Guidelines (the "guidelines") are intended to provide members of the Internal Auditors Society ("IAS") of the Securities Industry and Financial Markets Association ("SIFMA") with information for the purpose of developing or improving their approach towards auditing certain functions or products typically conducted by a registered broker-dealer. These guidelines do not represent a comprehensive list of risks and related work steps or procedures that can be followed during the course of an audit.

B. Objectives and Scope

The primary objective of these guidelines is to be used as a knowledge source to audit practitioners in developing their audit programs to test the design and operating effectiveness of internal controls over the risk of fraud in a broker-dealer. These guidelines are not designed or intended to serve as a broker-dealers' audit program over fraud risk. These guidelines may also be used to evaluate the broker-dealer's entity level anti-fraud programs and controls and in conducting your organization's fraud risk assessment. For purposes of these guidelines, fraud is defined as the intentional misrepresentation, concealment, or omission of the truth for the purpose of deception or manipulation to the detriment of a person or an organization. Fraud can be perpetrated by employees and non-employees of an organization.

Since many fraud controls also mitigate other risks, most key functions/activities of a broker-dealer organization are referenced in these guidelines. For example, the potential audit work steps relating to unauthorized sales and trading would most likely be part of your trading desk audit procedures.

When using these guidelines please note the following:

- These guidelines do not purport to include all risks within a broker-dealer relating to fraud that should be assessed by an audit practitioner;
- This is not an exhaustive set of procedures/audit work steps that audit practitioners need to follow during an audit of controls over the risk of fraud in a broker-dealer. For example, general fraud risks relating to insurance, payroll and procurement are not addressed in these guidelines;
- All work steps included may not be applicable to your organization;
- The absence of known fraud does not mean fraud is not occurring in your organization;
- Always verify explanations received from management even those received from seasoned employees;
- Understanding the organization across processes and activities is critical in identifying possible anomalies.
- Audit practitioners must consider factors such as the firm's risk and exposure with respect to size, business lines, customer base and geographic location in determining the appropriate procedures; and
- Audit practitioner should be familiar with current laws, regulations, and guidance materials including the following:

(1) Foreign Corrupt Practice Act (FCPA) (1977)
(2) Securities and Exchange Commission Guidance to Management Regarding Internal Controls Over Financial Reporting (2007)
(3) United States Sentencing Commission, Organizational Guidelines (USSG) (2004)
(4) Financial Industry Regulatory Authority (FINRA) Sanction Guidelines (2007)
(5) IIA Auditing Standards and Fraud Guide (2009)
(6) AICPA Guidelines
(7) Association of Certified Fraud Examiners' Guidance
(8) Regulations and Principles of the U.S. Department of Justice
(9) U.S. Federal Acquisition Regulations
(10) U.S. Sentencing Commission
(11) Public Company Accounting Oversight Board ("PCAOB")
(12) Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management Framework Foreign Corrupt Practice Act (FCPA) (1977)
(13) Other specific country regulations where business is conducted (e.g., UK Bribery Act)

C. Guideline Organization

These guidelines have been organized into two sections 1) General anti-fraud audit guidelines and 2) Specific broker-dealer anti-fraud audit guidelines.

For each section, the following elements have been included:
(i) Risks to be Managed;
(ii) Types of Controls to Managed/Mitigate the noted risks; and
(iii)Potential Audit Work Steps which could be deployed by the audit practitioner.

It should be noted that there may not be a direct alignment of the risk, control and potential audit steps in each section. Further, the above elements have been organized into topical sections and subsections to assist the audit practitioner in developing their audit approach with respect to fraud.

sifma

Internal Auditors Society

II. GENERAL ANTI-FRAUD AUDIT GUIDELINES

Included in this section are **general anti-fraud audit guidelines** including risks to be managed, types of controls to manage the noted risk and potential audit work steps which the audit practitioner could follow. This section is organized into the following topical sections:

This is not an exhaustive list of fraud risks and related audit procedures that audit practitioners need to follow during an audit of controls over the risk of fraud in broker-dealers. Further, not all procedures will be applicable to your organization. Audit practitioners must consider factors such as the firm's risk and exposure with respect to size, business lines, customer base and geographic location in determining the appropriate procedures. Further, the audit practitioner should be familiar with current laws, regulations, and guidance materials.

Risks to Be Managed	Types of Controls to Manage/Mitigate Risks	Potential Audit Work Steps
A. Board & Audit Committee Oversight:		
• The board or audit committee does not fully understand or exercise adequate oversight over internal control as it relates to fraud.	• The board or audit committee is knowledgeable about the content and operation, and exercises reasonable oversight with respect to the implementation and effectiveness of the: o Anti-fraud programs and controls, o Assessment of fraud risk, o Control activities over significant risks identified by the assessment, o Monitoring and auditing procedures to detect fraud, o Investigation of alleged or suspected misconduct, o Organization's information and communications programs, and o Remediation, when significant misconduct is discovered, including taking reasonable steps to prevent further misconduct or recurrence.	• Review the audit committee charter and documentation surrounding disposition of responsibilities under charter. • Review board of directors and/or audit committee meeting agendas and minutes for evidence of the oversight role being performed. • Attend board and audit committee meetings to observe the level of involvement of board and audit committee members in the oversight of anti-fraud activities. • Interview the chief audit executive, ethics and compliance officer, controller, head of SOX (if applicable) and external auditor regarding their interaction with the audit committee on matters involving fraud. • Assess whether the board and audit committee provide adequate oversight over: o Management's anti-fraud programs and controls, including monitoring and approving the organization's code of conduct, waivers of the code, the ethics hotline and whistleblower provisions, and the hiring and promotion of personnel in positions of trust or a significant role in the financial reporting process; o Assessment of fraud risk, including risk of fraud in their review of accounting principles, policies and estimates used by management and significant non-routine transactions entered into by management;

Risks to Be Managed	Types of Controls to Manage/Mitigate Risks	Potential Audit Work Steps
		○ Control activities over fraud risks identified by the assessment, including the risk of management override, collusion, unauthorized access and other circumvention; ○ Monitoring and auditing for fraud; ○ Investigation of alleged or suspected fraud; and ○ Remediation.
B. Management Oversight:		
• Management does not fully promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law or does not effectively implement programs and controls intended to prevent, detect and respond to external or internal fraud. • Operations, Finance and other "front line" personnel are not equipped with the appropriate knowledge, skills and tools to prevent, detect, and respond to fraud.	• Management, through communication, action and example, encourages ethical conduct and commitment to comply with applicable regulations and laws. • Management assigns overall responsibility to individuals who have substantial control over the organization or who have a substantial role in the making of policy within the organization, including directors, executive officers, or leaders of major businesses or functional units. • Management assigns day-to-day operational responsibility to high-level personnel or, individuals who exercise substantial supervisory authority. • Management takes reasonable steps to communicate periodically and in a practical manner the organization's standards, procedures and other aspects of the compliance, ethics and anti-fraud program.	• Obtain and review management's documentation regarding anti-fraud programs and controls. • Gain an understanding of how operations, finance and other "front line" personnel receive training and tools to prevent, detect and respond to fraud. • Interview executive and senior management, including CEO, CFO, chief legal counsel, business unit and function leaders and head of internal audit, regarding their role in implementing the organization's anti-fraud programs and controls. • Interview non-executive employees regarding their role, knowledge and skills regarding the organization's anti-fraud programs and controls. • Assess whether management's communication, action and example encourages ethical conduct and commitment to compliance with law. • Assess the "tone at the top" and whether it spreads up, down and across the organization.

Risks to Be Managed	Types of Controls to Manage/Mitigate Risks	Potential Audit Work Steps
C. Training:		
• Training regarding codes of ethics and conduct and key fraud risks and response strategies is nonexistent or ineffective.	• Comprehensive training materials which includes information regarding prevention, detection, investigation and remediation of fraud , identified risks, strengths and weaknesses of anti-fraud control activities, allegations of misconduct and remediation efforts. • Training includes function and product "Red Flags" that are sufficiently comprehensive for staff and management to identify potential fraud scenarios. • Training covers how suspected fraud situations should be communicated within the organization. • Training attendance is tracked.	• Obtain and review management's fraud training documentation, including training material and its comprehensiveness and lists of employees trained. • Conduct interviews to assess the effectiveness of the training program with the Chief Risk Officer, Chief Ethics Officer, and Human Resources. • Interview a range of employees from among different business units and functions to determine whether they have received anti-fraud training and their opinions as to its effectiveness, including whether they believe that they have received adequate training and tools for them to identify, prevent, detect and respond to fraud pertaining to their area of the organization. • Interview and assess competency of instructors.
D. Management Awareness & Communication:		
• Management awareness of fraud prevention and controls is not shared or communicated effectively. • Fraud, which could have been prevented or timely detected, recurs because the organization fails or does not adequately share information.	• Communication regarding anti-fraud policies and procedures flows down, up, and across the organization. • Effective management awareness facilitates communication of information, which includes collecting and sharing information regarding identified fraud risks, strengths, and weaknesses of anti-fraud control activities, incidents within the organization or at other organizations, and remediation efforts.	• Review corporate communications on anti-fraud policies and procedures, noting nature, frequency and method of communications. • Conduct interviews to determine how the organization shares information about fraud, including identified fraud risks, strengths and weaknesses of anti-fraud control activities, incidents at the organization or at other organizations and remediation effects. • Assess whether the organization: o Uses its information systems

Risks to Be Managed	Types of Controls to Manage/Mitigate Risks	Potential Audit Work Steps
		and technology as tools in the knowledge management process with regards to fraud; o Clearly communicate anti-fraud policies and procedures flow down, up and across the organization; o Allows upstream communications through someone other than a direct superior, such as an ombudsman or corporate counsel are available and maintained; o Permits anonymous communications and has implemented persons who have reported suspected improprieties to receive feedback; o Allows external parties to report ethical concerns or issues involving fraud; o Confirm communications are made to outside parties delivered by management level commensurate with the nature and importance of the message (e.g., senior executive periodically explains in writing the entity's ethical standards to outside parties); and o Confirm standards are reinforced in routine dealings with outside parties.
E. Code of Ethics & Conduct:		
• The organization has no code of conduct or the code of conduct is incomplete and fails to address conflicts of interest, related party	• The organization has implemented and publicized written standards that are reviewed and update annually that promotes an organizational culture of honest ethical conduct, including:	• Review the code of conduct for appropriateness and completeness of content and ensure they are reviewed and updated annually. • Interview employees across business units and functions to

Risks to Be Managed	Types of Controls to Manage/Mitigate Risks	Potential Audit Work Steps
transactions, illegal acts, and monitoring by management and the board.	○ Ethical handling of actual or apparent conflicts of interest between personal and professional relationships; ○ Full, fair, accurate, timely, and understandable financial reporting and disclosures in the periodic reports required to be filed by the organization; and ○ Compliance with applicable governmental rules and regulations.	assess the operating effectiveness of management's process of communicating the code and to determine whether individuals understand the entity's expectations as articulated in the code. • Determine whether and how the code is accessible to employees (e.g., inclusion in employee handbook, policy manual or on organization intranet.), including whether it is translated into foreign languages. • Review request for waivers of the code. • Confirm with multi-location firms, whether the same code is utilized at these locations and whether any modifications were required due to local laws and communicated. • Discuss with management and examine documentation to confirm that the standards in the code are communicated to third parties (i.e. customers and vendors). • If the code is communicated to third parties, consider including fraud-related questions on documentation such as accounts receivable confirmations. • Evaluate training curriculum and related materials regarding the code. • Evaluate whether the code clearly articulates what constitutes fraudulent behaviour and is updated or reviewed for updates on a periodic basis. • Confirm the codes explicitly states: ○ Who owns the compliance process; ○ Who is responsible for

Risks to Be Managed	Types of Controls to Manage/Mitigate Risks	Potential Audit Work Steps
		following-up on violations; o All employees are responsible for their own actions; and o All employees in all locations are subject to the same code. • Confirm the code applies to all employees and members of the board of directors or similar governing body to ensure that any observed instances of misconduct or pressure to compromise ethics standards are reported. • Confirm the code articulates how accountability for the codes is established and the sanctions imposed for non-compliance. (Employees believe that, if caught violating behavioural standards, they will suffer the consequences). • If the organization employs a confirmation process, review a sample of personnel files and assess whether the confirmation process and procedures address the following areas: o Whether all covered persons, including international persons, are subject to the same confirmation process; o How the organization knows that all covered persons have completed a confirmation; o If a member of management is designated to review all of the responses; o If the completed confirmations are stored safely; and o How exceptions are communicated to management and the audit committee.
F. Ethics Hotline / Whistleblower Program:		

Risks to Be Managed	Types of Controls to Manage/Mitigate Risks	Potential Audit Work Steps

• The organization has not implemented a system, including mechanisms allowing for anonymity or confidentiality, whereby employees, agents and other third parties may report or seek guidance regarding potential or actual fraud or other criminal conduct without fear of retaliation.
• The ethics hotline and whistleblower program is ineffective since it:
  ○ Lacks employee and external third-party awareness, encouragement of use, or appropriate and timely response;
  ○ Does not operate independently of management and with audit committee oversight;
  ○ Audit committee does not periodically review complaints submitted through the Ethics Hotline and Whistleblower Program.
	• The organization has implemented, publicized and documented procedures for the receipt, retention and treatment of complaints and confidential, anonymous submission of concerns by employees or third parties.
	• The audit committee has established procedures for receiving and retaining information about, and treating alleged incidents involving the organization regarding accounting, internal accounting controls or auditing standards and for confidential, anonymous submission of concerns by employees about questionable accounting or auditing matters such as an ethics hotline and whistleblower program.
	• The ethics hotline provides employees and third parties a means of communicating concerns, anonymously if preferred, about potential violations of the code of conduct, including unethical behavior and actual or suspected fraud or criminal conduct, without fear of retribution.
		• Review management's documentation regarding the ethics hotline/whistleblower program.
		• Determine whether a formal methodology exists for confidential, anonymous hotline reporting and appropriate follow-up.
		• Interview management and other employees regarding, as relevant, their:
		  ○ Awareness of the program and how information regarding the hotline is communicated to employees and third parties; and
		  ○ Understanding of how the process is managed and complaints are assigned, investigated, and escalated to senior management and the Audit Committee.
		• Review sample communications that promote the existence of an Ethics Hotline/Whistleblower Program.
		• Examine a sample of alleged incidents to obtain evidence to determine:
		  ○ How the complaint was addressed and resources assigned;
		  ○ How the complaint was resolved; and
		  ○ If there was appropriate and timely follow-up.
		• If third party provider operates hotline, conduct interviews with representatives of the provider to assess the quality of its operation, its protocols and scripts for speaking with complainants, process for categorizing and reporting complaints to

Risks to Be Managed	Types of Controls to Manage/Mitigate Risks	Potential Audit Work Steps
		organization's hotline manager, etc. • Consider pretext calls to hotline to assess how calls were initially handled by hotline operators and whether complaint is properly reported and investigated. • Assess whether the Audit Committee provides adequate oversight of the design of the Ethics Hotline & Whistleblower Program and review of complaint process. • Assess employees and third parties awareness of the Ethics Hotline/Whistleblower Program and determine their comfort level with the process including if reporting of alleged incidents is encouraged and if employees are using the hotline to get advice for difficult decisions. • Assess the communication channels for reporting financial-related complaints to the Audit Committee. • Evaluate the process for placing a complaint and processing a complaint including the competency of individuals executing the program and management's ability to avoid reporting complaints. • Assess whether a formal process exists to track issues as they are reported and track trends that may be emerging in one business area or across the business. • Assess whether statistics and trends are analyzed periodically, on a business-wide basis, to make certain that the ethics hotline/whistleblower program is functioning properly as well as to

Risks to Be Managed	Types of Controls to Manage/Mitigate Risks	Potential Audit Work Steps
		help identify trends that require further action, such as training course development and delivery. • Assess whether the program operates independently of management and if defined responsible parties that monitor the program who are independent from management (potentially independent third-party) or who are neutral parties within the organization (Ethics or Compliance Officer or Internal Auditor) and report to appropriate oversight party (Audit Committee). • If a third party administers the hotline, assess whether there is timely and appropriate monitoring of the third party service. • Assess whether the Audit Committee provides adequate oversight of the design of the Ethics Hotline & Whistleblower Program and review of complaint process.
G. Hiring & Promotion Procedures:		
• The organization fails to take reasonable efforts not to hire or promote into a position of substantial authority an individual whom the organization knew or should have known through the exercise of due diligence, has engaged in fraud, illegal activities or other conduct inconsistent with an effective anti-fraud, compliance and ethics program.	• Standards exist for hiring and promotion, including background investigations and maintenance of all information in the personnel files for all positions. A higher-level of investigation may be warranted for those employees of substantial authority and those employees in sensitive functions such as cash management, HR, payroll, etc. • Standards have been established for hiring and promoting the most qualified individuals, with emphasis on educational background, prior work experience, past accomplishments and evidence of	• Review documentation regarding the organization's process and procedures for hiring and promotion of individuals with a focus on those positions of substantial authority and "sensitive" functions. • Review a sample of files of individuals hired or promoted into positions of substantial authority and/or sensitive functions. • Conduct interviews of management and others regarding the process and procedures for hiring and promotion.

Risks to Be Managed	Types of Controls to Manage/Mitigate Risks	Potential Audit Work Steps
	integrity and ethical behavior, which demonstrates the entity's commitment to competent and trustworthy individuals. • Appropriate background investigations are performed on consultants and temporary employees.	• Evaluate how the organization performs background checks, including the nature of scope of background investigations completed for new employees, and individuals to be promoted into positions of trust. • Assess the process that the organization uses to assess the competency of individuals conducting the background investigation. • Assess whether the organization interviews independent references, and documents the results of the interviews including individuals contacted, level of inquiry including the references' level of interaction with the employee's previously demonstrated behaviours.
H. Mergers & Acquisitions, Joint Ventures, Agents, Vendors, Distributors, Customers and Other Strategic Third Party Relationships:		
• The organization enters into third party relationships with an organization or individual whom the organization knew or should have known through the exercise of due diligence, has engaged in fraud or illegal activities or other conduct inconsistent with an effective anti-fraud, compliance and ethics program.	• Standards exist for selecting and monitoring third party relationships, including identifying and assessing the fraud risks and developing preventive and detective controls to mitigate the risks including: o Background investigations prior to entering the relationships; o Contract provisions mandating compliance with law and organization's code of conduct and policies; and o Monitoring, including exercising third party audit rights.	• Review documentation regarding organization's process and procedures for entering into third party relationships. • Review a sample of files relating to third party relationships. • Conduct interviews of management and others regarding the process and procedures for selecting and monitoring third party relationships. • Evaluate whether the organization identifies and assesses fraud and criminal conduct risks arising from the third party relationship. • Assess whether the organization interviews independent references, and documents the results of the interviews including individuals

Risks to Be Managed	Types of Controls to Manage/Mitigate Risks	Potential Audit Work Steps
		contacted, level of inquiry including the references' level of interaction with the employee's previously demonstrated behaviors. • Assess whether the organization includes contract provisions requiring the third party partners to comply with the law and the organization's code of ethics and conduct. • Assess whether the organization reserves and periodically exercises audit rights.
I. Systematic Fraud Risk Assessment Program:		
• The risk assessment fails to assess fraud risk on a systematic basis. • Risk assessment process does not include input from various disciplines and levels of management. • Assessment does not include consideration of the risk of circumvention of controls or management over-ride. • The fraud risk assessment is not subject to active audit committee oversight. • Inadequate documentary evidence of management's risk assessment process and the audit committee's involvement and review. • The organization's risk assessment process does not include significant business units and	• The organization, with the active oversight of the audit committee or other governance authority, has assessed fraud risk on a systematic rather than haphazard or informal basis. • The risk assessment considers a range of schemes and scenarios, including: o Fraudulent financial reporting and disclosure; o Unauthorized receipts (e.g., antitrust, tax fraud, over - billing); o Unauthorized expenditures (e.g., commercial and public bribery); and o Misappropriation of assets and information (procurement fraud, revenue leakage, theft of proprietary information). • Fraud risk assessments expand upon traditional risk assessment, focusing on schemes and scenarios, including the risk of override, collusion and other circumvention of controls. • The organization tailors the risk assessment to appropriate level	• Confirm the potential for fraud is considered as part of the organization's enterprise risk assessment process or risk management program. • Obtain and review management's documentation regarding the fraud risk assessment scope and results. • Interview senior management (CFO, CEO), chief audit executive, chief compliance officer, audit committee members and business unit and function leaders regarding their understanding and role in the fraud risk assessment. • Determine how management selected the units and functions at which fraud risk assessments are conducted. • Gain an understanding of the authority level and experience of those charged with assessing fraud risk for the organization and assess appropriateness. • Determine if senior management including the board of directors is

Risks to Be Managed	Types of Controls to Manage/Mitigate Risks	Potential Audit Work Steps
functions.	within the organization, extending beyond the entity level and including significant business units and functions.	involved in the process. • Conduct walkthrough of process for conducting fraud risk assessments. • Assess whether fraud risk assessment considers (i) fraudulent financial reporting, (ii) unauthorized receipts and expenditures, (iii) unauthorized acquisition, use and disposition of assets, (iv) asset misappropriation, and (v) fraud by senior management, board members and other individuals with a significant role in the financial reporting process. • Assess whether the organization identifies fraud risk on a recurring basis and when special circumstances arise, e.g., merger and acquisition, expansion to new products and markets, corporate restructurings, etc. • Assess whether the assessment considers vulnerability to management override and potential schemes to circumvent existing control activities. • Assess whether the assessment considers incentives and pressures on management to commit fraud.
J. Detection & Monitoring:		
• The organization may not timely identify (i) risk factors (i.e. changes of circumstances which could change the inherent likelihood of fraud, occurring) or (ii) risk indicators (i.e. red flags that the scheme may be occurring).	Management monitors • risk factors that increase the likelihood of fraud occurrence, or risk indicators where "red flags" may identify that fraud is occurring; and • The quality and effectiveness of the anti-fraud programs and controls. • The organization has clear and known reporting channels for	• Assess management's processes and documentation for monitoring fraud risk factors, risk indicators, reporting channels and the quality and effectiveness of its anti-fraud programs and controls. • Interview senior management, members of the audit committee, chief audit executive, chief legal officer, chief ethics and

Risks to Be Managed	Types of Controls to Manage/Mitigate Risks	Potential Audit Work Steps
	employees to notify potential fraud instances.	compliance officer regarding the organization's procedures and processes for monitoring of fraud risk factors, indicators, and anti-fraud programs and controls. • Conduct a walkthrough of the monitoring and evaluation process.
K. Incident Response & Remediation:		
• The organization lacks a standardized procedure for tracking, reporting, responding, investigating and remediating allegations of fraud or criminal conduct.	• The organization has a standardized investigative process for responding to allegations or suspicions of fraud. Does not wait until frauds are detected to develop a process.	• Review documentation regarding organization's incident response and remediation process. • Review a sample of files relating to investigating and remediation allegations or suspicions of fraud or criminal conduct. • Conduct interviews of the chief legal counsel and deputies, chief ethics and compliance counsel, chief audit executive, human resources director, security director and others regarding the process for investigating and remediation allegations or suspicions of fraud or misconduct. • Assess whether the organization has a standardized and effective process and procedure for tracking, reporting, responding and, investigating allegations of fraud or criminal conduct. • Assess whether the organization has a standardized and effective process to prevent and timely detect a recurrence, including: o Taking appropriate disciplinary and legal action against primary and secondary wrongdoers; o Conducting forensic auditing to assess whether the wrongdoers engaged in other, unrelated wrongdoing or whether similar misconduct

Risks to Be Managed	Types of Controls to Manage/Mitigate Risks	Potential Audit Work Steps
		occurred elsewhere in the organization; o Conducting a root cause analysis; o Sharing information within the organization and, if appropriate, reporting incidents to law enforcement and other third parties; o Providing financial and other forms of restitution to those harmed; o Enhancing anti-fraud programs and control activities; o Updating the fraud risk assessment; and o Monitoring implementation of the remediation plan. • Consider whether the appropriate functions are involved in evaluating and assigning resources to investigate the allegation, including, but not limited to, legal counsel, ethics and compliance, internal audit, and human resources. • Consider whether the functions that perform investigations have standardized policies, processes and documentation requirements.

sifma

Internal Auditors Society

III. SPECIFIC BROKER-DEALER ANTI-FRAUD AUDIT GUIDELINES

Included in this section are **specific broker-dealer anti-fraud audit guidelines** including risks to be managed, types of controls to manage the noted risk and potential audit work steps which the audit practitioner could follow. This section is organized into the following topical sections and sub-sections:

This is not an exhaustive list of fraud risks and related audit procedures that audit practitioners need to follow during an audit of controls over the risk of fraud in broker-dealers. Further, not all procedures

will be applicable to your organization. Audit practitioners must consider factors such as the firm's risk and exposure with respect to size, business lines, customer base and geographic location in determining the appropriate procedures. Further, the audit practitioner should be familiar with current laws, regulations, and guidance materials.

Risks to be Managed	Types of Controls to Manage/Mitigate Risk	Potential Audit Work Steps
A. Sales & Trading:		
a) Unauthorized or Improper Sales and Trading		
Including but not limited to the following: • Trading in unauthorized products / sectors. • Post market close mutual fund orders. • Fraudulent contingent purchases. • Improper fee waivers • Late trading and improper after-hours or off-premises trading. • Schemes against counterparties. • Receiving payments/kickbacks for trade flow that is undisclosed or inappropriate. • Selling unsuitable securities. • IPO Spinning. • Marking the close / open • Unauthorized side letter agreements. • Flash trading in breach of SEC regulations (proposed). • Improper crossing of trades • "Double-dipping," net trading. • Wash trades • Excessive mark-ups on fixed income securities or non-commission based trades. • Manipulation of the Treasury bond auction process. • Use of stale benchmarks to manipulate trade execution price.	• Clearly defined delegation of authorities for trading activities including a comprehensive listing of authorized products by trader. • Clearly defined and documented trading rules and strategies that are communicated to and understood by all traders. • Frequent supervisory review of all trading activity including trading performance, mark-up/down reviews, large dollar amounts, P&L attribution analysis, etc. • Comprehensive trading limits (including gross trading risk) and independent limit monitoring and escalation procedures. • Monitoring of appropriate key risk and performance indicators (KRIs and KPIs) by trading supervisors and independent risk management. • Segregation of duties among front, middle and back office personnel. • Periodic recertification of system access and entitlements. • Supervisory review procedures for cancellation, correction, rebooking and omission of trades.	• Review written desk trading policies and procedures and ensure that strategies are well defined and documented. • Verify if desk trading policies and procedures have been communicated to and understood by traders. • Confirm trading limits, approved products and parameters exist and are monitored by supervisors to identify inappropriate trading levels and activities. • Review trading limits and other monitoring reports, compare against trading strategy, and assess adequacy. • Determine if performance against the established parameters (e.g., limits, KRIs, KPIs) is monitored and regularly evaluated. Exceptions are logged and reviewed by management. • Verify that supervisors are adequately reviewing exception reports, supervising all trading activity and that issues are escalated as necessary. • Evaluate the segregation of duties between trade execution, trade capture, trade support, and trade cancellations and corrections. • Evaluate supervisory review of segregation of duties. • Verify that system access and entitlement recertification is performed on a periodic basis and is properly performed. • Ascertain that employee internal transfers are reviewed for excessive entitlements and terminated users have been disabled. • Review cancelled and corrected trades

Risks to be Managed	Types of Controls to Manage/Mitigate Risk	Potential Audit Work Steps
• Internal trades made at misrepresented or inflated values. • Recording fictitious trades to circumvent net trading risk limits. • Late booking of trades to circumvent trading risk limit reports. • Manipulation of the trade confirmation process to conceal fraudulent trades or trades against customer instructions. • Manipulation of the futures trade matching process to conceal fraudulent trades. • Improper cancellation, correction, rebooking or omission of trades. Recording trades into uncleared suspense accounts or other accounts that aren't affirmed/confirmed with counterparties. • Unauthorized trading. • Guaranteeing against a loss. • Recording fictitious trades at period-end to generate additional commissions. • "Stuffing the channel". • Broker rebates not properly allocated. • Intentional override or circumvention of customer instructions. • Manipulation of common reference data identifiers used in complex trades/structures to avoid being flagged for complex trade review.	• Thorough and independent trade confirmation process. • Timely and complete futures trade matching process. • Intercompany account reconciliations. • Reconciliation breaks escalation/discussion process between control groups. • Suspense and 'No-flow' accounts monitoring and resolution. • Clearly documented customer instruction policies and restricted access to customer and reference data to non-trading personnel. • Edit reports that identify reference data identifiers that have been recently/frequently altered. • Adherence with and monitoring of mandatory annual vacation policy. • Independent set-up of firm trading accounts. • Independent review of trading accounts not mapped to the firm's P&L and risk systems. • Flash Crash and Algorithmic trading preventative and detective controls.	and unconfirmed trades to identify unusual items or trends and verify follow-up conducted. • Review suspense and intercompany account reconciliations for adequate resolution of breaks. • Assess the adequacy of confirmation and affirmation processes. • Assess customer instruction policies and verify that management has a process in place to identify and monitor for instruction changes. • Determine who has access to change/update customer instructions and if there is an independent review • Assess policies for modifications to reference data identifiers. • Determine if senior management monitors compliance with the vacation policy (normally 10 consecutive business days by personnel who can enter or confirm trades and their supervisors) and if appropriate measures are taken in cases of non-compliance. Look for patterns of behavior in cases of non-compliance. • Review process to open and map firm trading accounts to P&L and risk systems. • Review adequacy of management controls around flash crash and algorithmic trading risk.

Risks to be Managed	Types of Controls to Manage/Mitigate Risk	Potential Audit Work Steps
b) Inaccurate Re-Pricing of Securities		
• Use of stale benchmarks to manipulate trade execution price. • Use of non-independent pricing sources to price verify securities. • Internal trades made at misrepresented or inflated values. • Trader overrides of independent price feeds.	• Clearly documented re-pricing policies and procedures. • Segregation of duties between traders and re-pricing. • Stale pricing report that identifies securities that have not been recently/frequently priced. • Additional trade monitoring for securities with infrequent re-pricing. • Report that lists manual changes/updates to pricing and comparison to independent/third-party pricing. • Exception reports that highlight trades outside normal pricing parameters and large day over day changes in prices. • Supervisory review of all trading activity. • Review of related party transactions (i.e. between subsidiaries) to verify that market prices have been given for all transactions.	• Assess re-pricing policies and verify that management has a process in place to identify and monitor stale pricing, price changes/overrides or other re-pricing anomalies. • Assess adequacy of segregation of duties between traders and re-pricing and associated access controls. • Assess adequacy of independent price verification process. • Review and assess pricing override procedures. • Assess the adequacy of pricing feeds and Service Level Agreement—assuming vendor pricing feeds. • Review adequacy of exception reporting, monitoring and follow-up. • Assess procedures for valuing complex structured products and illiquid investments.
c) Insider Trading		
• Employees trading or investing on non-public information (including front-running) whether for personal or firm benefit. • Ethical information barrier violations. • Trading in restricted entities.	• Clear policies on personal trading and prohibiting insider trading. • Clearly defined and documented trading policies and strategies. • Policies and controls over safeguarding of confidential	• Review the Personal Trading Policy and verify that all staff is aware of the Personal Trading Policy. • Verify if desk trading policies and procedures have been communicated to and understood by traders. • Verify that an annual affirmation is signed by all affected employees.

Risks to be Managed	Types of Controls to Manage/Mitigate Risk	Potential Audit Work Steps
• Aiding and abetting fraudulent third-party trading schemes.	information, such as segregation of duties and information wall restricting access to only necessary people. • Required employee disclosure of investment accounts- including any related accounts where the employee has an interest and/or has the power directly or indirectly to make investment decisions. • Pre-approval for personal trading. • Review of personal and firm trading activity by supervisors/ Compliance. • Trade surveillance reports to monitor for front running, piggybacking, and best execution. • Employees are prohibited from effecting a transaction involving a security covered by a research report, market update or other communication, whether written or oral, having market significance, until such time that such information is completely disseminated to customers. • Electronic and paper communication surveillance to detect insider trading policy violations. • Whistle-blowing anonymous hotline. • Security watch lists, preapproval lists and other reporting lists.	• Review written desk trading policies and procedures and ensure that strategies are well defined and documented. • Determine if monitoring against established parameters is regularly evaluated and that any identified exceptions are logged and reviewed by management. • Verify that electronic and paper communication reviews are performed on a periodic basis which applies an appropriate test sampling methodology, key word detection, and escalation process. • Review the accuracy of various watch lists and preapproved security lists.

Risks to be Managed	Types of Controls to Manage/Mitigate Risk	Potential Audit Work Steps
d) Conflicts of Interest		
• Putting the firm's interest ahead of customers. • Favorable treatment to related parties (subsidiaries, employees, and other related parties). • Putting the brokers/traders interests ahead of customers; • Utilizing vendors that do not offer the best pricing and value for services rendered. • Issuance of a fraudulent and/or misleading research report to benefit the firm ahead of a customer.	• Clear employee guidelines regarding conflicts of interest. • Employees must complete an annual statement of outside business interests. • Legal or Compliance should assess the business for potential conflicts of interest and create a log of all identified items for monitoring. • All related party transactions (i.e. between subsidiaries) should be independently reported and reviewed to verify that fair market prices have been given for all transactions. • Segregation of duties and information wall restricting information only to necessary people. • Physical and system information barriers between Research, Sales, and Trading teams. • Access to privileged and confidential information is restricted.	• Review the process management has established to identify and review for potential conflicts of interest. • Review intercompany transactions (i.e. between subsidiaries) and verify if all transactions have been reported and reviewed. • Determine if an adequate process has been implemented to determine fair pricing for related party transactions. • Assess the adequacy of information barriers and monitoring for potential conflicts of interest. • Review adequacy of personal trading policies and test compliance.
e) New Accounts		
• Traders intentionally not obtaining credit and compliance approval prior to trading. • Knowingly trading with unauthorized counterparties. • Failure to comply with required Know Your Customer ("KYC"), Client	• Segregation of duties between traders and back office personnel settling transactions with counterparties. • Independent set up of new accounts. • Documented KYC, CIP, PEP and OFAC procedures	• Review account opening and KYC, CIP, PEP and OFAC policies and procedures. • Assess adequacy of segregation of duties among front and back office personnel. • Review counterparty credit approval and limit monitoring processes. • Verify that policies and procedures

Risks to be Managed	Types of Controls to Manage/Mitigate Risk	Potential Audit Work Steps
Identification Program ("CIP"), Politically Exposed Persons (PEP) and Office Foreign Asset Control ("OFAC") laws and regulations.	for all new accounts. • Trading supervision. • Independent counterparty credit limit reporting and monitoring. • Daily monitoring of trading activity by independent risk management.	regarding P.O. Box addresses, address changes, hold mail and escheatment are properly controlled and supervised. • Review procedures for restricting trading to authorized counterparties.
f) Securities Lending		
• Breach of fiduciary responsibility to institutional investors and/or favoring one client over another. • Customers who lose money in securities lending claim they did not understand the risks and the dealer should not have allowed them to lend or borrow securities. • Failing to disclose the true nature and risks associated with the securities lending program resulting in artificially inflated stock prices and potential investor litigation. • False finder's fees and illegal kickbacks. • Other improper or unauthorized securities lending activity (see controls above on Improper or Unauthorized Sales and Trading). • Excessive or minimal rebates paid/received. • Excessive lending to or borrowing from a counter party (concentration risk).	• Know your customer policies and procedures. • Trading supervision. • P&L attribution analysis and customer profitability analysis. • Brokerage fee analysis. • Counterparty verification procedures to ensure traders are appropriately authorized to trade on behalf of the counterparty. • Signed customer agreements with appropriate terms and conditions clearly explaining risks. • Controls to ensure trading with authorized counterparties only. • Trading limits aligned with risk appetite that are monitored and enforced. • Early warning indicators to identify and escalate changes in risk profile. • Monitoring for off-market rebates.	• Review account opening and KYC policies and procedures. • Review a sample of customer agreements for appropriateness of contract terms, disclosures and customer suitability. • Review counterparty verification procedures. • Review trading supervision and performance reporting and monitoring, including P&L attribution analysis and counterparty concentration analysis. • Assess adequacy of oversight of trading activities by independent risk management including monitoring of limits, KRIs, KPIs and other early warning indicators of changes in risk profile. • Evaluate rebate monitoring procedures.

Risks to be Managed	Types of Controls to Manage/Mitigate Risk	Potential Audit Work Steps
B. Theft of Assets:		
a) Cash		
• Employee or counterparty theft of cash. • Check kiting (recording a fraudulent payment). • Theft of checks, payments, premiums, commissions, fees, etc. • Fictitious vendors, counterparties, and customers. • Overstating cash. • Inappropriate use of suspense, unclaimed assets, dormant, or error accounts. • Record bank transfers as cash payments from customers.	• Written policies and procedures. • Multiple levels of review and approval when opening and closing cash accounts. • Reconciliation of GL to bank statements. • Physical counts of any cash held at the company. • Limited access to cash and checks. • Documentation to support movement of cash and checks. • Segregation of duties (check signers do not have access to blank checks or update the GL and reconciliations performed by independent person). • Mandatory employee vacations and rotation of duties. • Controls over the receipt of checks including immediate restrictive endorsements ("for deposit only"). • Limited edit access to the GL. • Maintenance of a log to record incoming checks prior to deposit. • Code of ethics and whistle-blowing anonymous hotline. • Documented signing authorities and duplicate approvals for large dollar disbursements.	• Conduct an analytical review of cash including changes and trends in balances and relationships with other accounts. • Analyze key ratios such as current ratio (current assets to current liabilities); quick ratio (current assets i.e., inventory and prepaids to current liabilities), and cash to total assets. • Review reconciliation performed to agree cash, re-perform the reconciliation, and investigate any open items. • Confirm financial statements auditors obtain independent confirmations from the bank directly for key cash accounts. If they do not, confirm balances directly with banks. • Evaluate segregation of duties for key duties related to cash – reconciliations, access to blank checks, issuing checks and updating the GL. • Review voided checks and supporting documentation. • Review check approval process and confirm physical checks obtained the necessary signatures. • Review insurance coverage for cash activities. • Review the payees for checks and compare to an authorized vendor list. • Confirm checks paid are supported with appropriate documentation for the purpose of the payment. • Confirm blank check stock is kept in a secure area (locked cabinet or safe) and review staff with access. • Confirm checks prepared for payment pending signature or mailing are also kept in a secure location with staff access limited. • Evaluate the process for returned

Risks to be Managed	Types of Controls to Manage/Mitigate Risk	Potential Audit Work Steps
		checks. • Investigate any missing checks that were not voided or paid and processed. • Review deposits in transit and confirm they were promptly recorded by the bank in subsequent statements. • Review the process for depositing checks or cash for adequate segregation of duties. • Review a list of payees on non-payroll checks and addresses and compare to the firm's employee database to identify and investigate matches. Investigate any payments to employees and confirm appropriateness. • If numerous or large checks are issued, review cancelled checks for potential tampering such as inferior paper stock, alterations, payees that do not reconcile to AP, signatures not matching individual signatures, unauthorized check signers, the use of signature stamps, duplicate payments, and missing documentation.
b) Wire Transfers		
• Unauthorized wire transfers sent. • Wire transfers sent to the wrong counterparty or for the wrong account. • Wire transfers sent to a third party not properly screened for Office of Foreign Asset Control ("OFAC").	• Written policies and procedures. • Segregation of duties. • Mandatory employee vacations and rotation of duties. • Separate preparer and approver required for all wires. • Payments over established thresholds are independently reviewed and approved. • Documented call back procedures for wires. • Access to wire payment systems is restricted to only required employees. • Passwords for wire systems are required to be changed and are encrypted.	• Review the controls over wire transfers (should be similar to cash). • Review supervisory controls for funds transfers. Verify that payments over established thresholds are independently reviewed and approved. • Determine that access to wire payment systems is restricted. • Evaluate password controls for wire transfer systems. • Review insurance coverage for wire transfer activity. • Confirm callbacks for wire transfers are requested for payments over certain thresholds. • Evaluate suspicious activity monitoring processes. • Verify that third party wire transfers are screened against the OFAC restricted list.

Risks to be Managed	Types of Controls to Manage/Mitigate Risk	Potential Audit Work Steps
	• Payments are monitored for suspicious activity (e.g., recurring payments to one counterparty without a valid business purpose, payments to one counterparty from multiple client accounts). • Third party wire transfers are screened for OFAC purposes.	
c) Accounts Receivable (AR)		
• False financial invoices received from a counterparty or vendor. • Fictitious vendors, counterparties, and customers. • Employee or counterparty theft. • Overstating AR. • Not reporting rebates or allowances (adjustment to receivable if not a liability). • Understate allowance for doubtful accounts. • Failure to write off uncollectible AR. • Customer disputes or returns not recorded or investigated. • Record fictitious AR or overstate amount. • Fail to provide refunds or discounts owed to customers. • False refunds or discounts. • Skimming or stealing a portion of customer payments. • Lapping or applying payments to different customer accounts to conceal fraud. • Failure to have an effective	• Written policies and procedures. • Vendor due diligence. • Segregation of duties between access to funds and recording of AR. • Appropriate supervision. • AR account reconciliations. • Approvals for adjustments, any unusual entries or write-offs. • Monitor accuracy of allowance for doubtful accounts. • Mandatory employee vacations and rotation of duties. • Code of ethics and whistle-blowing anonymous hotline. • Tracking and following up on aged AR balances.	• Conduct an analytical review of receivables including changes and trends in balances and relationships with other accounts. • Analyze key ratios such as current ratio (current assets to current liabilities); quick ratio (current assets i.e., inventory and prepaids to current liabilities), current assets to total assets. • Review a sample of receivables and the payment process. • Investigate possible red flags such as transfers of credits between customers, delays to posting customer payments, missing customer remittance advices, undocumented credit adjustments, customer inquiries about unapplied payments, large past due balances, etc. • Investigate entries to alter activities such as credits, voids, returns, dormant credits, etc. • Assess segregation of duties between the receipt of funds and recording of AR. • Identify any dormant accounts and investigate activity. • Perform an independent confirmation with customers unless performed by financial statement auditor. • Review the receipt of payments on AR and handling of incoming payments through the mailroom to the AR department.

Risks to be Managed	Types of Controls to Manage/Mitigate Risk	Potential Audit Work Steps
collection process on aged AR balances.		• Review aged AR and confirm customers with past due amounts are notified (addresses are correct) and they are aware of this status. • Analyze refunds, returns, and allowances for appropriateness. • Compare dates of customer payments with the dates payments are posted to customer accounts (to detected lapping). • Verify that an effective tracking and follow up process exists for aged AR balances.
d) Marketable Securities & Investments		
• Fictitious vendors, counterparties, and customers. • Employee or counterparty theft. • Overstating marketable securities and investments. • Knowing use of bad data or prices from third parties. • Over-billing by a vendor for an asset.	• Written policies and procedures. • Segregation of duties among access to securities, record keeping and reconciliation. • Counterparty due diligence. • Reconciliations to front office and brokers. • Mandatory employee vacations and rotation of duties. • Independent market values and price calculations by the back office. • Review by a valuation committee or investment group. • Documented policies and procedures to govern models used to calculate derivatives market values or other illiquid or hard to price securities. • Code of ethics and whistle-blowing anonymous hotline.	• Conduct an analytical review of marketable securities and investments including changes and trends in balances and relationships with other accounts. • Analyze key ratios such as marketable securities to total current assets. • Confirm duties are segregated. • Review and re-perform reconciliations. • Review pricing process and confirm from independent sources. • Review policies and procedures and approval processes for valuation models. • Confirm pricing differences and exceptions are identified and resolved promptly. • Confirm the valuation process and portfolio is reviewed by the financial statement auditors. • Review senior management oversight through a valuation committee or other method.
e) Payroll		
• Fictitious employees. • Unauthorized compensation. • Improper allocation of	• Written policies and procedures. • Segregation of duties.	• Conduct an analytical review of payroll including changes and trends in balances and relationships with other

Risks to be Managed	Types of Controls to Manage/Mitigate Risk	Potential Audit Work Steps
expenses between affiliates.	• Employee set-up on payroll systems requires supervisory review and is independent of payroll payment process. • Mandatory employee vacations and rotation of duties.	accounts. • Evaluate process for setting up new employees. • Compare changes in payroll to budget and investigate large differences. • Confirm that the segregation of duties for handling payroll is appropriate.
f) Property, Plant and Equipment		
• Misappropriation of equipment. • Employee or counterparty theft. • Overstating property, plant, and equipment. • Over-billing by a vendor for an asset. • Flipping of real estate or other asset to inflate value. • Retiring assets below market value. • Cost of asset exceeds fair value. • Assets acquired for personal not business use. • Assets acquired to bribe customers or politicians. • Long term leases that are not appropriate to the business. • Related party transactions at off market prices. • Over-billing and kickback schemes.	• Written policies and procedures. • Security and monitoring procedures for equipment and other property that can be removed. • Approval process and documentation requirement for purchases, sale, and retirement of property, plant, and equipment, including multiple approvals for higher priced items. • Periodic evaluation of business need for existing property, plant and equipment. • Sale or retirement process to ensure fair value and arms length transactions. • Bidding and review process for additions and renovations to property, plant and equipment. • Code of ethics and whistle-blowing anonymous hotline.	• Conduct an analytical review of property, plant, and equipment including changes and trends in balances and relationships with other accounts. • Compare changes in property, plant, and equipment to budget and investigate large differences. • Confirm inter-company or related party assets purchased or transferred have an independent valuation or appraisal and confirm payment (cash or payable) was recorded correctly. • Select a sample of assets and confirm existence and current usage. • Calculate relationships between fixed assets and other accounts such as fixed assets/total assets, fixed assets to long term debt, depreciation expense to fixed assets, and accumulated depreciation to fixed assets. • Confirm a sample of property, plant and equipment in use and supported with adequate documentation. • Review the depreciation periods and calculations for accuracy. • Compare changes in property, plant, and equipment to budget and investigate large differences.
g) Intangible Assets		
Note: Two primary forms of intangibles are analyzed: (1) legal intangibles such as trade secrets, copyrights, patents,	• Written policies and procedures. • Maintain security of customer lists and	• Conduct an analytical review of intangible assets including changes and trends in balances and relationships with other accounts.

Risks to be Managed	Types of Controls to Manage/Mitigate Risk	Potential Audit Work Steps
trademarks, and goodwill; and (2) competitive intangibles such as human capital and related activities: • Receipt of stolen intellectual property. • Employee or counterparty theft. • Overstating intangible assets. • Theft of intellectual property.	competitive proprietary information. • Require confidentiality agreements when discussing information with third parties. • Require non-compete agreements with key employees. • Conduct due diligence on all front office hires. • Code of ethics and whistle-blowing anonymous hotline.	• Review supporting documentation for intangibles booked as assets. • For intangibles booked to the financial statement, confirm review by the financial statement auditors. • Review competitive intangibles and how these are monitored and protected such as through confidentiality and non-compete agreements and the code of ethics. • Evaluate the security of key information such as models, customer lists, proprietary information, etc.
h) Other Assets		
• Improper capitalization of expenses as assets (such as start up costs, marketing costs, salaries, research and development costs, etc. that should be expensed). • Manipulating inter-company accounts or transactions • Overstating other assets.	• Written policies and procedures. • Maintenance of supporting documentation to clearly indicate expenses that were capitalized and the rationale. • Documented management approval for capitalized amounts. • Review and feedback from accounting policy staff or external auditors if unusual or questionable. • Code of ethics and whistle-blowing anonymous hotline.	• Conduct an analytical review of other assets including changes and trends in balances and relationships with other accounts. • Confirm deferred charges and capitalized items have future benefits that are identifiable. • Confirm compliance with GAAP requirements and review by financial statement auditors. • Confirm that other firms typically capitalize these types of assets.
C. Code of Conduct/Compliance Violations:		
a) IT Security Violations		
• Inappropriate access to confidential information and/or live trading applications. • Front office personnel access to middle office systems or books and records to conceal trading losses. • Unauthorized persons access trading desk systems and/or confidential information,	• Defined list of security violations/ toxic access combinations. • Access to applications, databases and data files is granted based on job function and supports segregation of duties. • Applications authenticate user prior to granting access. • Unsuccessful login attempts	The following steps focus on fraud risk and are not a complete set of procedures for conducting an IT audit: • Evaluate process to define and maintain toxic access combinations. • Evaluate process for identifying, reporting and following up on users identified with toxic access combinations. • Review users of applications, databases

Risks to be Managed	Types of Controls to Manage/Mitigate Risk	Potential Audit Work Steps
causing trading losses and/or information breach. • Improper change to counterparty account data as a result of inappropriate system access. • Violation of privileged access rights. • Firewall violations. • Unauthorized personnel make program system changes. • Trading activities are halted or interrupted due to an intentional system outage. • Network/systems penetrated through illegal hacking.	are reported. • Access is revoked for terminated users and employees transferring to departments where access is not required. • Access and entitlements are recertified semi-annually. • Audit trail exists for access to confidential information and are sent to management for review. • Privileged user access is logged and periodically reviewed. • IT developers do not have standing access to production applications or data; emergency access is logged and approved. • Update access to production source code and scripts are restricted to development team. • Production changes following change management procedures requiring code scans, testing and multi-level sign off. • A fault tolerant platform including redundancy and fail over. • Penetration testing is periodically performed to identify and resolve network/systems security vulnerabilities.	and data files and confirm that access and entitlements is based on job function. • Evaluate the entitlement levels support segregation of duties. • Confirm that the same user is prevented from entering, reviewing and approving the same transaction, including across applications. • Evaluate adequacy of application, database and data file provisioning process including appropriateness of approvers. • Confirm application and databases require verifying identity of user prior to granting access. • Confirm that passwords for applications follow information security policies including complexity and resets. • Confirm application locks users out after a predetermined amount of unsuccessful login attempts. All unsuccessful login attempts are logged and reported to information security. • Evaluate process for revoking accounts for terminated users and recertifying access for users who transfer to other departments or change job function. • Evaluate process for recertifying application; database and data file access and entitlements semi-annually. • Evaluate that applications are classified correctly and handle restricted data according to the CIS Policy including restricting all levels of access and masking of data prior to copying data to non-production environments. • Confirm that all activity, including privileged user activity, to restricted data is logged in an audit trail and sent to Information Owners and Information Security for review. • Review process for IT developers to request access to production, including during non-working hours. Verify that

Risks to be Managed	Types of Controls to Manage/Mitigate Risk	Potential Audit Work Steps
		all access is logged and approved. • Verify that update access to production source code is granted to members of the development team. Access is revoked for terminated accounts and recertification is required for users who transfer to other departments or change job functions. • Confirm that all production changes require approvals from business and IT, vulnerability code scans and adequate testing prior to implementation. • Verify that ability to migrate production changes is restricted to appropriate members of the Change Management group. • Verify that network/systems penetration testing is periodically performed by qualified personnel and that security weaknesses identified are promptly addressed.
b) Improper or Undue Influence		
• Senior management overrides of appropriate controls. • Undue influence over trading support functions of the firm. • Improper gifts, gratuities, and entertainment. • Improper business expense claims.	• A whistleblower hotline that can be used by and is communicated both internally (i.e. to all employees) and externally (i.e. to all third parties such as vendors, agents, etc.). • Detailed policies and procedures relating to travel and entertainment expenses, gratuities and gifts, in accordance with applicable regulations (i.e. FINRA Rule 3020). • Provide fraud awareness and ethics related training to employees and other relevant stakeholders. • Segregation of duties within all key/ critical trading support functions. • Independent review and	• Conduct audit of the whistleblower hotline by determining whether complaints were properly investigated and closed. • Perform hotline benchmarking by comparing metrics and statistics (such as call volume) with publicly available industry standards/averages. • Check records showing the attendance at ethics and compliance/fraud trainings and determine whether all relevant employees and departments attended. In addition, review training materials for appropriate coverage and content. • Determine that policies related to gifts, gratuities and travel and entertainment expenses are in place and comply with applicable regulations. • Conduct periodic audit of actual entertainment and other related expenses (invoices, other support and reasons for the expenses) to ensure

Risks to be Managed	Types of Controls to Manage/Mitigate Risk	Potential Audit Work Steps
	authorizations of entertainment expenses and other business expenses. • Independent review and authorization of business claims before they are reimbursed. • Certification by employees in which they represent that business expense claims being requested were incurred for valid business reasons in accordance with the organization's gratuities, gifts and travel and entertainment expense policy.	compliance to policies and procedures. Validate that such expenses were incurred for relevant business reasons. • Test journal entries for appropriate approvals and accounting treatment. • Make inquiries of relevant personnel to discuss: o Knowledge of any incidents of improper or undue influence, including override of controls; o Understanding of the policies and procedures relating to travel and entertainment expenses, gratuities and gifts; o Risks and red flags of improper or undue influence, including override of controls; Programs and controls management has designed and implemented to prevent and detect improper and undue influence, including override of controls.
c) Improper Business Activity		
• Fraudulently reducing an entity's tax liability by transferring monies from offshore to onshore entities to fund activity. • Antitrust activities. • Round trip transactions. • Improper labor practices. • Immigration and naturalization offenses. • Environmental, health and safety violations.	• A whistleblower hotline that can be used by and is communicated both internally (i.e. to all employees) and externally (i.e. to all third parties such as vendors, agents, etc.). • Provide fraud awareness and ethics related training to employees and other relevant stakeholders. • Independent review of the organization's tax liability calculation. • Independent monitoring of transfers of monies between entities. • Policies on antitrust activities, labor practices, immigration and naturalization activities and	• Conduct audit of the whistleblower hotline by determining whether complaints were properly investigated and closed. • Perform hotline benchmarking by comparing metrics and statistics (such as call volume) with publicly available industry standards/averages. • Check records showing the attendance at ethics and compliance/fraud trainings and determine whether all relevant employees and departments attended. In addition, review training materials for appropriate coverage and content. • Review tax liability calculations, including supporting documents, for appropriateness and compliance with the accounting policies and procedures. • Test a sample of monies transferred between entities for appropriate application of company policy and

Risks to be Managed	Types of Controls to Manage/Mitigate Risk	Potential Audit Work Steps
	environmental health and safety rules. • Excessive trading policy including definition of roundtrip transactions and consequences for those that execute such transactions. Communication of this policy to employees (e.g. trainings, emails, etc.). • System notification for trades that may be indicative of round trip transactions. Timely review and follow up of such notifications. • Constant communication to relevant stakeholders about the organization's policy on antitrust activities, labor practices, immigration and naturalization activities and environmental health and safety rules. • Emphasis on ethics and integrity and zero tolerance fraud policy that is regularly communicated to employees via mechanisms such as newsletters, emails, etc.	procedure. For any transfers from offshore to onshore entities, perform inquires and request supporting documentation. • Determine that policies related to antitrust activities, labor practices, immigration and naturalization activities and environmental health and safety rules are in place and are appropriately worded. • Determine that policies related to excessive trading including definition of roundtrip transactions are appropriately worded with appropriately consequences for non-compliance. • Review communication to employees on 1) zero tolerance for fraud and 2) emphasis on ethics and integrity as part of company culture. • Review communication to relevant stakeholders on the organization's policy on antitrust activities, labor practices, immigration and naturalization activities and environmental health and safety rules. • Testing of activities relating to antitrust, labor, immigration and naturalization and environmental health and safety to ensure that a) items were in accordance with the relevant company policy and b) that any exceptions or violations were investigated and closed in a timely and appropriate manner. • Testing of trading activity for compliance with excessive trading policy and round trip transactions. Review of system notifications of transactions that may be round trip in nature, including whether such cases were investigated and closed in a timely and appropriate manner. • Make inquiries of relevant personnel to discuss: o Knowledge of any incidents of

Risks to be Managed	Types of Controls to Manage/Mitigate Risk	Potential Audit Work Steps
		improper business activity; o Understanding of the policies and procedures relating to roundtrip transactions, antitrust activities, labor practices, immigration and naturalization activities and environmental health and safety rules; o Risks and red flags of improper business activity; and o Programs and controls management has designed and implemented to prevent and detect improper business activity.
d) Misrepresentation		
• Malicious spreading of unsubstantiated rumors. • Improperly licensed personnel conduct business on behalf of the Firm (e.g., unlicensed traders, unlicensed sales assistants). • CV and academic deception.	• Policies and procedures prohibiting the dissemination of rumors in accordance with applicable regulations [i.e. NYSE Rule 435(5)] • Communication Policies • Code of Ethics / Code of Ethics training • Phone recording • Email review policies and procedures • Compliance testing program • Management oversight • On boarding attestations • Credentials verification process for new hires	• Confirm policies and procedures are in compliance with regulatory requirements, current, accessible, and communicated and training is provided. • Confirm that on boarding attestation related to responsibilities around communication exist. • Confirm phone conversations are maintained – review samples. • Confirm that an email review program is in place, that sample sizes are adequate. Test for compliance. • Review access and monitoring controls for social media tools (e.g., Twitter, Facebook). • Verify that employees receive training on firm policies on Code of Ethics, Communications with the Public, Social Media, etc.). • Determine if a compliance testing program is in place and registrations are confirmed against job responsibilities. • Confirm that a management review process exists to determine whether staff registrations and license requirements are adequate and current for each position. • Confirm that background checks and CV data points and accreditations are

Risks to be Managed	Types of Controls to Manage/Mitigate Risk	Potential Audit Work Steps
		verified.
D. Financial Information, Reporting & Disclosure:		
a) Business Combination, Intangibles - Goodwill and Others		
• Goodwill on acquisition incorrectly appropriated to reporting units. • Reporting units not fully complying with "Segment Reporting" guidance under Topic 280. • Goodwill not pushed down to the right reporting unit level. • Fair value cash flow assumptions for reporting units inaccurate or falsified. • Discount rate assumptions are manipulated to get favorable results. • Book value computation of reporting units intentionally falsified to pass "Step 1" test. • Impairment indicators (e.g., recurring losses or declining revenue prospects) intentionally overlooked. • Incorrect determination of useful life of intangible assets.	• Compliance with Topic 350 of GAAP codification. • Supervision and review of the accounting for business combinations and the consolidation process, focusing on the risk of a reasonable possibility of a fraud occurring. • Maintenance of documentation supporting fair value determinations. • Supervisory review of the appropriateness of assumptions and other data inputs used in fair value measurements. • Assessment and measurement of business/economic developments that could lead to asset impairments. • Supervision of asset sales classified as assets held for sale or discontinued operations.	• Ensure that reporting units are consistent with segment disclosure assessment. • Ensure that assumptions used in the valuation of reporting units is reasonable and observable. • Depending on the complexity, consider using a specialist in the valuation of the reporting units. • Ensure that the projected cash flow information of the reporting units is obtained from reliable sources within the organization. Consider segregation of duties between the accounting department and the source of projected cash flow data. • Obtain information on reporting units from independent sources to determine if impairment could be triggered.
b) Investments - Debt, Equity and Derivatives		
• Misclassification of securities as trading, available-for-sale, held-to-maturity or held for investment resulting from fraudulent intent and earnings management. • Investments in securities and derivative transactions are made but are not authorized.	• Compliance with Topic 320 and 815 of GAAP codification. • Documented policies and procedures.	• Obtain evidence of intent of classification as trading, available-for-sale, or held-to-maturity. • Consider using the work of a specialist in determining the fair value of the securities or derivatives, and scrutinize the specialist's qualifications, integrity, and results. • Verify the fair value of securities using multiple brokers or third parties.

Risks to be Managed	Types of Controls to Manage/Mitigate Risk	Potential Audit Work Steps
• Investments and derivatives are valued incorrectly. • Unreasonable or unsupportable fair value estimates. • Unauthorized pledging of investments occurs for the benefit of employees or third parties. • Impairment issues are not timely identified or correctly measured. • Fictitious investments. • Management manipulating its assertion at the inception of the hedge that the hedging relationship will be highly effective. • Using inter-company derivatives to manage earnings, designation of non-derivatives as hedging instruments and inappropriately applying the hedge criteria.		• Ensure that management is not aggressive in the use of assumptions in valuation of illiquid investment. • Verify that complete and accurate information is being provided to independent pricing vendors to ensure that they have the requisite data to independently price the positions. • Evaluate the legitimacy and financial viability of the custodian when confirming investments, including verifying the proper address of the custodian. • Insist on inspecting original supporting documents rather than copies, e.g., original security certificates, brokers' statements, etc. • Expand tests of details and trace all transactions to the appropriate accounts. • Trace sales proceeds and investment income to bank or brokerage statements. • Trace cost of investment purchases to cancelled checks and bank statements. • Review all journal entries related to investments and derivatives and examine supporting documents. • Scrutinize and investigate investments acquired in exchange for non-cash assets or company stock. • Ensure that GAAP requirements for hedge accounting are strictly applied.
c) Investments - Equity Method and Joint Ventures		
• Manipulation of the "significant influence criteria" for equity method investments to obtain the desired accounting treatment and financial results.	• Compliance with Topic 323 of GAAP codification. • Investments in all limited partnerships should be accounted for using the equity method unless the investor's interest "is so minor that the limited partner may have virtually	• Inquire with management as to whether the entity has the ability to exercise significant influence over the operating and financial policies of the investee • Evaluate the attendant circumstances that serve as a basis for management's conclusions.

Risks to be Managed	Types of Controls to Manage/Mitigate Risk	Potential Audit Work Steps
	no influence over partnership operating and financial policies." Investments of more than 3 to 5 percent are considered to be more than minor.	
d) Loan Loss Reserves and Provisions		
• Loan loss methodologies are not well documented. • Overrides exits making top level adjustments possible without clear or adequate explanation. • Allocated and unallocated portion of the loss not clearly documented. • Different categories of loans are aggregated together to distort information. • Disclosure made with the intent to mislead investors. • Overstate the amount of provisions (also referred to as "cookie jar reserves") to cover the expected costs of liabilities such as taxes, litigation, bad debts, job cuts and acquisitions. • Establishment of inflated accruals in those years where the company is extremely profitable and can afford to incur larger expense amounts. These "cookie jar reserves" are then tucked away for management to reach into and reverse in future years where the company is unprofitable or marginally profitable when a boost to earnings would be beneficial.	• Loan loss provision percentages are reviewed and approved periodically for validity. • The portfolio is reconciled to supporting documentation to ensure that information is transferring completely and accurately. • The reserve for loan loss required balance calculations are reviewed for accuracy and approved by senior management. • The loan loss reserve balance is reviewed for adequacy on a periodic basis.	• Ensure that the loan loss provision has been developed with a disciplined methodology. • Ensure there is adequate documentation for the loan loss provision. • Mechanism to reduce differences between estimated and actual observed losses should be documented.

Risks to be Managed	Types of Controls to Manage/Mitigate Risk	Potential Audit Work Steps
e) Software Development Costs (for internal use)		
• Inappropriate basis for capitalization. • Costs are capitalized that are not in accordance with GAAP. • Capitalized amounts are not timely written off in order to boost earnings.	• Ensure compliance with Topic 350 of GAAP codification.	• Assess systems in place to track software developments costs. • Cost capitalization commences when an entity has completed the conceptual formulation, design, and testing of possible project alternatives, including the process of vendor selection for purchased software, if any. Auditors should consult with the company's technical personnel (i.e. engineers, programmers) in reviewing management's assertions that technological feasibility has been achieved. • In order to justify capitalization of related costs, it is necessary for management to conclude that it is probable that the project will be completed and that the software will be used as intended. Test for adherence. • When it becomes no longer probable that the computer software being developed will be completed and placed in service, the asset should be written down to the lower of the carrying amount or fair value, if any, less costs to sell. Test for adherence.
f) Revenue Recognition		
• Improper revenue recognition either prematurely or of fictitious nature. • Side agreements agreed to outside the normal reporting channels of the business having an effect on revenue. • Channel stuffing -- practice of offering concessions to clients to induce rendering of service in the current period, when they would not have been otherwise sold	• Compliance with SEC Staff Accounting Bulletin 101, Revenue Recognition in Financial Statements, ("SAB 101"). • Access controls for making changes to pricing files is restricted to individuals with such designated job responsibilities. • Supervision of the ability to create or change credit limits and payment terms is restricted to credit personnel	• Obtain and review evidence that a trading arrangement exists. • Obtain and review evidence that associated services has been rendered. • Review contracts to determine if seller's price to the buyer is fixed or determinable. • Assess organization's ability to collect payment. • Test significant transactions at quarter end and year end to ensure revenue was appropriate. • Perform analytical procedures that to highlight potential revenue trend

Risks to be Managed	Types of Controls to Manage/Mitigate Risk	Potential Audit Work Steps
until later periods, if at all.	and approved by management. • Management review and approval for all orders with pricing overrides. • The collections group monitors the A/R to identify changes in payment-term trends.	anomalies.
g) Improper Capitalization of Expenses		
▪ Capitalization of certain costs for nonrefundable fees associated with lending, committing to lend, or purchasing a loan or group of loans. This technique allows a company to capitalize and amortize the expense over many periods rather than recognize it in its entirety in the current period.	• Compliance with GAAP topic 340	• Review capitalization policy to assess if the company is overly aggressive with its practices compared to its peers. • Obtain and assess management's reasons for selecting the policy including appropriate approvals. • Assess if the costs items are providing future benefit thereby warranting capitalization. • Sample test a selection of items that have been capitalized to ensure they are reasonable and in line with policy. • Review capitalized items for appropriate approvals in line with policy.
h) Reorganization Charges		
• Expense charge that are not in accordance with GAAP. These could be a "big bath" type expense or an under accrual of the charge.	• Compliance with GAAP topic 852	• Obtaining assurance that the reorganization plan is approved and the basis of charge is reasonable evidenced and appropriately approved.
i) Compensations - Stocks		
• Stock option backdating.	• Ensure compliance with GAAP Topic 718.	• Ensure that controls are in place with respect to the option registers and that there is adequate governance and segregation of duties in the compensation department. • Test key controls.

Risks to be Managed	Types of Controls to Manage/Mitigate Risk	Potential Audit Work Steps
j) Compensation - Retirement Benefits		
• Assumptions underlying pension computation are not supportable.	• Ensure compliance with GAAP Topic 715.	• Where necessary, consider using the work of a specialist to review the reasonableness of assumptions.
k) Income Taxes		
• Tax planning strategies for tax evasion. • Improper basis for deferred tax assets. • Inadequate disclosures on uncertain tax provisions.	• Ensure compliance with GAAP Topics 340 and 740.	• Where necessary consider the use of a specialist. • Ensure that projected income data for deferred taxes is reliable and consistent with other projected data used for budgetary purposes. • Obtain data of pending tax litigations.
l) Improper or Inadequate Disclosures and Misclassifications		
• Misrepresent the financial condition of the company through misstatements and omissions of the facts and circumstances that explains the financial data in its financial reporting. • Misrepresentations, intentional inaccuracies, or deliberate omissions in management discussions and other non-financial statement sections of annual reports, 10-Ks, 10-Qs, and footnotes to the financial statements. • Improper classifications of line items in the income statement with the intention to mislead the investor.	• Controls are in place to ensure Compliance with GAAP and SEC disclosures requirements	For public companies, refer to the SEC Interpretative Release No. 33-8350, Commission Guidance Regarding Management's Discussion and Analysis of Financial Condition and Results of Operations. The audit program should consider the following steps: • Test to ensure that financial statement disclosures have been reviewed and approved by senior individuals from finance, reporting and legal. • Inquire of external auditor to gain an understanding of how they obtain comfort on financial statement disclosures. • Review any last minute significant changes to disclosures/classifications for reasonableness. • Considering independently assessing disclosures against the standards; • Read the disclosure and financial statements to ensure they include all key transactions, etc. based on your understanding of the organization. Further, inquire of management where disclosures are unclear and/or ambiguous. • Review the accounting policies included in the footnotes to determine if

Risks to be Managed	Types of Controls to Manage/Mitigate Risk	Potential Audit Work Steps
		any of the policies could be considered aggressive and not in line with industry practice.
m) Disclosure of Loss Contingencies		
• Loss contingencies are not accrued but are disclosed in the financial statements. • Deliberately not disclosing or providing inadequate disclosure.		• Consult the legal department and obtain their representation. • Review supporting documentation for the disclosure of loss contingencies.
n) Related Party Transactions		
• Transactions between related parties where either little or no consideration is given for the product or service. • Relationships intentionally not made transparent. • Lack of persuasive evidence of an arm's length arrangement. • Failure to adequately	• Compliance with GAAP Topic 850. • Clear policies and procedures for identifying and properly accounting for related party transactions. • Loan receivable and guarantees are clearly documented, including the nature of the relationship of	• Conducting public records searches/background investigations on customers, suppliers and other individuals to identify related parties and confirm legitimacy of business. • Performing data mining to determine whether transactions appear on computerized files. • Performing document review of identified transactions to obtain

Risks to be Managed	Types of Controls to Manage/Mitigate Risk	Potential Audit Work Steps
disclose the nature and amounts of related party relationships and transactions. • Borrowing or lending on an interest-free basis or at a rate of interest significantly above or below market rates. • Selling real estate at prices that differ significantly from appraised value. • Exchanging property for similar property in a non-monetary transaction. • Loans with no scheduled terms for when or how the funds will be repaid. • Loans with accruing interest differing significantly from market rates. • Loans to parties lacking the capacity to repay. • Loans advanced for valid business purpose and later written off as uncollectible. • Non-recourse loans to shareholders.	the guarantor to the reporting entity. • The process for reconciling inter-company accounts is clearly defined and documented. • Inter-company accounts are reconciled on a monthly basis and reviewed and approved by senior management.	additional information for further inquiry. • Searching for unusual or complex transactions occurring close to the end of a reporting period. • Reviewing the nature and extent of business transacted with major suppliers, customers, borrowers and lenders to look for previously undisclosed relationships. • Reviewing confirmations of loans receivable and payable for indications of guarantees. • Performing alternative procedures if confirmations are not returned or returned with material exceptions. • Reviewing material cash disbursements, advances and investments to determine if the company is funding a related entity. • Testing related party sales to supporting documentation (i.e., contract and sales order) to ensure appropriately recorded. • Discussing with counsel, prior auditors and other service providers the extent of their knowledge of parties to material transactions. • Inquiring about side agreements with related parties for right of return or contract cancellation without recourse.

Internal Auditors Society