Internal Audit Guidelines

Electronic Communication

August 2008

TABLE OF CONTENTS

I. INTRODUCTION AND BACKGROUND.....2

II. AUDIT GUIDELINES.....12

III. GLOSSARY.....48

I. Introduction and Background

I. INTRODUCTION AND BACKGROUND

A. Overview

Electronic messaging (e.g., e-mail, chat, instant messaging, bulletin board, and blogs) has revolutionized the manner in which Firms conduct business and communication by providing a common, streamlined method of electronic communication and increasing the efficiency, quality, and productivity of the workplace. Many businesses utilize e-mail and instant messaging as means of communication both internally as well as with external clients. Emerging technologies have extended access to e-mail from the desktop computer to wireless devices, such as Blackberry hand-held devices.

B. Regulatory Background

There are numerous rules, guidelines, and regulations regarding electronic messaging from various governing bodies that member firms must comply with. These regulations include the Securities Exchange Commission (SEC) Rules 17a-1 and 17a-4, FINRA-07-59, Rule 204-2 and Rule 206(4)-7of the Investment Advisors Act of 1940, NASD Rule 3110 and NYSE Rule 440.10. Generally compliance with the more stringent SEC Rules 17a-1 and 17a-4 will ensure compliance with most of the other regulations.

Rule 17a-4 is a rule created by the SEC under the Exchange Act that stipulates specific record keeping requirements for certain exchange members, brokers, and dealers in the securities industry. The Rule was updated in 1997 to expressly allow for the storage, retention, and reproduction of records by means of “electronic storage media,” subject to certain conditions.

SEC Rule 17a-4 impacts individuals and organizations that trade or act as brokers for traders that sell. This includes any financial institution whose business units trade securities regulated by the SEC and FINRA. Compliance with Rule 17a-4 requires that members, brokers and dealers carefully evaluate their information management processes and architecture to ensure that the relevant records and communications are maintained in a trustworthy state for the duration required by the Rule, and that they are retrievable for review on demand for the time required. In light of this, organizations subject to the Rule’s requirements that do business electronically may need to implement new technologies to comply.

Pursuant to SEC Rule 17a-4, broker-dealers are required to preserve for a period of not less than three years, the first two years in a readily accessible place, "originals of all communications received and copies of all communications sent by [the broker-dealer] relating to [its] business as such." To achieve compliance with Rule 17a-4, originals of all incoming correspondence relating to the firm’s business and copies of all outgoing correspondence must be retained by the reviewing supervisor in the appropriate correspondence file, in each case for at least three years.

In 1997, the Commission amended paragraph (f) of Rule 17a-4 to allow broker-dealers to store records electronically in a "non-rewriteable, non-erasable format." Under the Rule, electronic records must be preserved exclusively in a non-rewriteable and non-erasable format. This interpretation clarifies that broker-dealers may employ a storage system that prevents alteration or erasure of the records for their required retention period.

While SEC Rule 17a-4 largely focuses on exchange members, brokers, and dealers, it is also applicable to those organizations that are classified as a Self-Regulatory Organization (SRO), i.e., national securities exchanges, national securities associations, registered clearing agencies and the Municipal Securities Rulemaking Board. In addition to SEC Rule 17a-4, these SROs are required to be in compliance with SEC Rule 17a-1. The main difference between the two rules is that 17a-1 requires the document preservation period, in general, to be not less than five years, the first two years in an easily accessible place, unless special permission is granted by the SEC.

The following guidelines from FINRA-07-59 are also applicable to electronic messaging systems. These include risk-based procedures to review electronic communications as follows:

1. Flag electronic communications that may evidence or contain customer complaints, problems, errors, orders or other instructions for an account; or evidence conduct inconsistent with FINRA rules, federal securities laws and other matters of importance to the member's ability to adequately supervise its business and manage the member's reputational, financial and litigation risk.

2. Identify such other business areas the member may identify as warranting supervisory review.

3. Educate employees to understand and comply with the member's policies and procedures regarding electronic communications.

Adopting such supervisory review procedures requires firms to:

- Identify the types of correspondence that will be pre- or post-reviewed.

- Identify the organizational position(s) responsible for conducting reviews of the different types of correspondence.

- Monitor the implementation of, and compliance with, the member's procedures for reviewing public correspondence.

- Periodically re-evaluate the effectiveness of the member's procedures for reviewing public correspondence and consider any necessary revisions.

- Provide that all customer complaints, whether received via e-mail or in other written form, are reported to appropriate regulatory bodies in compliance with reporting requirements.

- Prohibit employees from the use of electronic communications unless such communications are subject to supervisory and review procedures developed by the firm.

- Conduct necessary and appropriate training and education.

Investment advisory firms should also be aware of the following additional and applicable regulatory requirements with respect to electronic communications.

The Investment Advisors Act of 1940 ("the Advisors Act") requires the registration of investment advisors with the SEC. Rule 204-2 of the Advisors Act, "Books and Records to be Maintained by Investment Advisers," specifically details e-mail creation and retention requirements for all client records. This rule details the types of books and records an Advisor must make and keep true, current and accurate for their business. E-mail is specifically identified as a business record in the rule. Section (g) of 204-2 sets specific rules for retention, non-rewriteable storage, and ease of retrieval and viewing, including preservation "in an easily accessible place for a period of not less than five years, the first two years in an appropriate office of the investment adviser." Rule 204-2 further requires investment advisors to arrange and index the records in a way that permits easy location, access, and retrieval of any particular record and to promptly furnish to the SEC any records requested, electronic or otherwise.

SEC Rule 206(4)-7 also requires Advisers to adopt and implement policies and procedures reasonably designed to prevent violation of the Advisers Act. Such policies and procedures must be written and designed to prevent violation of the Investment Advisers Act of 1940 by the Adviser and its supervised persons (which includes any partner, officer, director, or employee of an Adviser, or other person who provides investment advice on behalf of the Adviser and is subject to the supervision and control of the Adviser). The Advisors Act explains that a firm's policies and procedures should take into consideration the nature of its operations and be designed to prevent, detect and promptly correct material violations of the Advisers Act. It is important to note that under the rule compliance is an ongoing process that requires the review, updating, and amendment of such policies and procedures including the controls for reviewing e-mail and safeguards for the protection of client records and information.

Additionally firms are also reminded that they have a separate, but equally important, obligation to ensure that their use of electronic communications media enables them to make and keep records as required by NASD Rule 3110 and NYSE Rule 440.10. The Financial Industry Regulatory Authority (FINRA) has issued a document entitled *"Guidance Regarding Review and Supervision of Electronic Communications document (FINRA 07-59)"* that can be used to assist firms with compliance to all applicable regulations regarding electronic communications. This document may be found at:

http://www.finra.org/RulesRegulation/NoticestoMembers/2007NoticestoMembers/P037553

C. Audit Objective

An electronic messaging audit will determine the quality and effectiveness of the organization's infrastructure, services, and associated software that support the firm's electronic communication systems. The audit will disclose the adequacy of the global electronic communication systems with respect to regulatory requirements, the safety and soundness of the system, and the planning process for the firm to maintain, resume, and recover electronic communication operations.

While many of the regulatory requirements and guidelines of the SEC and FINRA for both Broker Dealers and Investment Advisors overlap or are redundant; the objective of the audit is to address the most stringent aspects of the regulations. Therefore, coverage for less stringent and overlapping requirements is implied.

The objectives of the audit are to ensure that:

- The firm is in compliance with external regulatory and reporting requirements.

- Management has assumed responsibility for formulating, developing, documenting, promulgating, and controlling electronic messaging policies, and that procedures are in place to determine that the policies are being followed.

- System security is adequate to safeguard electronic messaging information against unauthorized use, disclosure or modification, damage or loss and that appropriate physical security and access control measures have been established.

- Management has taken appropriate and timely action to address the deficiencies noted in prior audit and examination reports.

D. Audit Scope

The audit review will focus on how the electronic communication systems are configured and implemented to comply with the applicable regulatory requirements. The scope of the audit will include the following areas:

- Documented policies and procedures.

- Regulatory compliance as it pertains to retention, media storage, security and availability of electronic communications.

- Regulatory compliance for internal business communications (i.e., which departments are blocked from communicating with one another).

The focus of the audit will also cover the following requirements of Rule 17a-4 or 17a-1:

- Members, brokers and dealers "preserve for a period of not less than three years (or five years per 17a-1 for SROs), the first two years in an easily accessible place originals of all communications received and copies of all communications sent that are related to their business as broker-dealers, including electronic communications such as e-mail and instant messaging.

- Electronic media used to store these records preserve them "exclusively in a non-rewriteable, non-erasable format" such as WORM (Write Once Read Many) technology.

- The electronic storage media automatically verifies the quality and accuracy of the storage media recording process and that original and duplicate messages are fully indexed and searchable.

- Members, brokers and dealers have specific electronic records available for SEC review at all times for immediate, easily readable projection or reproduction.

- The member, broker or dealers store separately from the original, a duplicate copy of the original record on any medium acceptable for the time required.

In summary, these audit guidelines focus on those factors that present the greatest degree of risk to the firm and at a minimum will include the following areas:

- Overall Scope
- Organizational Structure and Management
- Electronic Communication Policies and Standards:
- Compliance
- System Architecture and Configuration
- System Administration
- System Security
- System Monitoring
- System Operation and Support
- Business Continuity
- Archival, Retention and Retrieval
- Review of Third Parties Providing Archival Services
- Service Level Agreements and Contracts
- Message Content Supervision
- Prior Audit Issues
- Conclusions and Action Plan

These audit guidelines do not address other audit risks associated with electronic communications such as security over e-mail and other external data transmissions and network access points outside of a member firm's control that may be intercepted, compromised or otherwise exploited by unauthorized parties, malicious software or viruses.

D. Audit Risks

Failure to comply with global, federal, state, and local regulations could cause a firm to be fined or prevented from communicating electronically by regulators thereby impacting business operations. If the technology supporting the electronic messaging environment is also not properly aligned to meet regulatory requirements, the firm can be subject to additional fines and penalties.

Audit risks are summarized as follows:

Organizational Structure and Management

Failure to establish responsibility for engineering and operating of the electronic communication services along with a defined structure to enable clear reporting lines and communication to upper management may result in required electronic communications not being captured and stored properly thereby placing the firm in a non-compliance situation.

Electronic Communication Policies and Procedures

Establishing electronic communication policies and procedures alone does not guarantee the smooth flow of messages. Each individual in the organization must be aware of the rules and procedures that apply to him. The damage that can result from inadequate knowledge of existing policies and procedures could result in delays in electronic communication, compromised or lost messages, or viruses and other malicious software that could disrupt the entire electronic communications infrastructure. An awareness program and periodic training are required to minimize these risks and keep the electronic communication services operating at maximum levels.

Compliance

Compliance issues may arise if management is unaware of or does not fully understand regulatory requirements regarding electronic communications or if oversight of the electronic communications infrastructure is not sufficient to ensure compliance.

System Architecture and Configuration

Unapproved, unprotected, and/or unnecessary electronic communication services could waste system resources, degrade a server's performance and down time, and more importantly create critical security loopholes. Unnecessary and unapproved IP-Services should be removed.

System Administration

Failure of system administrators to deal with the moving target and subsequent liabilities of license compliance, configuration changes, monitoring user profiles and user access, auditing user sessions, and modifying administration settings could result in system breaches by unauthorized users and/or software that could cause corruption of messages, overwhelming inbound spam, use of the system to generate outbound spam, installation of viruses and other malicious software, and loss of or degradation of electronic communication services.

System Security

Security breaches may result in the use of the electronic communication facilities to send out unauthorized messages thereby damaging a firm's reputation. They may also cause the loss or damage of archived messages that could place the firm in violation of regulations or allow the introduction of malicious software that could impede the performance of the electronic communication network.

System Monitoring

Management oversight and monitoring of critical electronic communication operations is essential. The lack of audit logs and active monitoring may result in unauthorized breaches of the electronic communication infrastructure.

System Operation and Support

Inadequate support for production job processing could cause either a failure of the electronic communication infrastructure. Lack of capacity planning and monitoring that result in inadequate space to store messages required by regulation could cause compliance issues. Computers and network performance should also be monitored and analyzed to ensure that they can support critical jobs and a regular analysis of performance metrics is required to identify bottlenecks and improve electronic communication performance.

Equipment maintenance of the computers, network, and telecommunications equipment that support electronic communication is critical to the smooth running of messaging operations. Performing regularly scheduled maintenance which includes cleaning, checks and updates on equipment will help prevent system problems instead of waiting for failures to occur. Risks mitigated by having a scheduled maintenance program for electronic communication equipment include equipment outages, costly repairs, excessive down time, and loss of data that may all potentially impact business operations and/or compliance with regulations.

Business Continuity

A Business Continuity Plan ("BCP") that addresses electronic communication enables a firm to survive a disaster and to re-establish critical communications required to support the business within the timeframes set out by business managers. A disaster could result in short-term or long-term delays in message processing.

An electronic communication BCP should address the following risks:

- Ensure that electronic communication recovery is covered in both the firm's overall BCP as well the firm's data center or third party service provider's BCP.

- The development, implementation, testing and maintenance of business continuity and emergency response plans that enables the firm to protect its communication assets and meet its business recovery objectives.

- Addresses a process for reconstruction of archived electronic communications as well as the infrastructure and services that will be needed to resume electronic communications in the event that the primary services are destroyed or unavailable for a long period of time.

Archival and Retrieval

Back-up and recovery procedures may not be in place to ensure that the company can recover from any form of messaging failure or the loss of individual records. The procedures for backup and recovery need to be reviewed from the standpoint of day-to-day backup and contingency planning as well as regulatory compliance for the retention of electronic communication messages.

Back-up copies of all data may not be made on a regular basis to ensure that the data can be restored in as complete a manner as possible in the event of a processing failure. Back-up copies may not be stored off-site in order to ensure that they are not destroyed by the same disaster that requires them to be used for recovery purposes.

Review of Third Parties Providing Archival Services

Outsourcing continues to be a key part of many firms' cost management strategy particularly with respect to e-mail and other forms of electronic communication. The strategy has proven to be effective but brings with it significant risks that must be recognized and managed since a firm's reliance on third parties may adversely impact certain business functions. If not properly managed, outsourcing of electronic communications may negatively affect a firm's operations and clients. The service can be outsourced, but the risk cannot. Some of the potential negative outcomes may include:

- On-time delivery performance and end customer satisfaction levels may decline because of delays at third party processing sites.
- Product or service quality may suffer.
- Suppliers may not be financially viable.

Service Level Agreements and Contracts

It is critical to clearly define the roles and responsibilities of third party service providers, software providers, and licensors to manage the ongoing relationship between the firm and the vendor. More often than not, however, a firm's expectations of the relationship are not clearly defined. In fact, in many cases, management may not completely understand the obligations and commitments of an electronic communication vendor. Therefore, firms should use a well defined service level agreement as a tool for managing the risks associated with outsourcing and to agree upon practices for managing, measuring, and monitoring vendor performance.

Message Content Supervision

An audit of electronic communication procedures for financial firms must also address a member firm's obligations to supervise electronic communications based on the content and audience of the message in addition to the electronic exchange and recordkeeping requirements for messages to ensure that they are reasonably designed to achieve compliance with applicable federal securities laws and self-regulatory organization (SRO) rules. Risks in this area include customer complaints that go unreported or unaddressed and prohibited and privileged business discussions that could place in a member firm in violation of federal securities laws.

At one time, FINRA required that members review all correspondence of their registered representatives pertaining to the solicitation or execution of any securities transactions. In 1998, recognizing that the growing use of electronic communications such as e-mail made adherence to this requirement difficult, FINRA amended its rules to allow members the flexibility to design supervisory review procedures for correspondence with the public that are appropriate to the individual member's business model.

In considering this guidance, members generally may decide by employing risk-based principles the extent to which the review of incoming, outgoing and internal electronic communications is necessary in accordance with the supervision of their business. However, members must have policies and procedures for the review by a supervisor of employee's incoming, outgoing and internal electronic

communications that are of a subject matter that require review under FINRA rules and federal securities laws.

Prior Audit Issues

An effective audit process includes a firm's commitment to addressing issues that arise out of prior electronic communication audits and therefore all audits should include a review of these follow-up activities. An individual or small group from the firm should be designated with the authority and responsibility to follow-up and report on progress towards implementing all prior audit recommendations through coordination with appropriate management. They should also fulfill the obligation to communicate the implementation status of prior audit recommendations to executive sponsors, EC management, and internal auditors. This individual or small group should also be accountable to ensure implementation efforts fully resolve audit issues or findings on a timely basis. Failure to follow-up and resolve prior audit issues may impair a firm's ability to meet regulatory compliance obligations for electronic communications and messaging.

II. Audit Guidelines

II. AUDIT GUIDELINES

Risk To Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
A. Overall Scope		
Lack of awareness around factors that present the greatest degree of risk to the firm with respect to electronic communications and the need to meet regulatory requirements, the safety and soundness of the system, and the planning process for the firm to maintain, resume, and recover electronic communication operations in order to support critical business operations.	Determine examination scope and approach for reviewing electronic communications.	• The scope, objectives, and approach will be discussed with management prior to commencing the review. • Diagrams will be required to document the electronic communication infrastructure and services in order to understand the features of the system and who, where, and how they are executed as preparation for an audit. • Testing controls will generally be by inquiry, observation and inspection. However, some sample testing of electronic communication procedures may be required to corroborate that control procedures are being applied. • Identify relevant regulatory and statutory requirements. • Review past reports for outstanding issues or previous problems. Consider: – Regulatory reports of examination; – Internal and external audit reports; – Business continuity test results; and – Organization's overall risk assessment and profile. • Review management's response to issues that rose since the last audit. Under consideration will be: – Adequacy and timing of corrective action; – Resolution of root causes rather than just specific issues; and – Existence of any remaining outstanding issues.

Risk To Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		• Interview management and appropriate electronic communication operations staff to identify: – Any significant changes in business strategy or internal business processes that could affect the operation of electronic communications; – Any material changes in the audit program, scope, or schedule related to electronic communication activities; – Key management changes; – Information technology environments and changes to electronic communication configuration or components; – Changes in key service providers (e.g., messaging, archival and retrieval, and back-up/recovery); and – Any other internal or external factors that could affect the electronic communication process. • Determine management's consideration of newly identified threats and vulnerabilities to the organization's electronic communication process. Consider: – Technological and security vulnerabilities; – Internally identified threats; and – Externally identified threats (including known threats published by information sharing organizations). • All audit issues raised during the current examination will be discussed and approved with management and include responses prior to report issuance.

Risk To Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
B. Organizational Structure and Management		
Lack of clear responsibilities for the management and operation of electronic communication services that could result in security, compliance, and other issues that impact a firm's ability to conduct business.	A defined structure to enable clear reporting lines and communication to upper management. Skilled resources to support and operate the electronic communications infrastructure.	• Review and assess organizational charts and functional roles: – Clear assignment of responsibilities; – Reporting lines; and – Segregation of duties. • Review experience level of staff in relation to electronic communications services (e.g., MS-Exchange) in use at the firm. • Determine if staff have a minimum level of experience and there are ongoing training plans in place to ensure that all staff have the requisite skill sets. • Verify with management the level of staffing, staff turnover rates, and the use of consultants to ensure adequate levels of experienced staff are maintained on a regular basis. • Obtain and review organization charts for the IT and Compliance groups; identify key personnel and their responsibilities as it relates to electronic communications.

Risk To Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
C. Electronic Communication Policies and Standards		
A lack of established policies and procedures over the electronic communication environment can result in inappropriate administration and support (i.e. insufficient resources, poor management, and/or inappropriate architecture) as well as regulatory requirements not being effectively understood by all business stakeholders and relevant support groups.	Appropriate policies and standards are in place regarding electronic communication (e.g., e-mail, instance messaging, message board, Blogs, and Chat) that are compatible with firm policies. Policies and procedures should be communicated adequately to the persons concerned. An implementation plan should be defined for the adaptation of existing infrastructure to the policy requirements.	• Obtain and review all relevant electronic communication (e.g., e-mail, instance messaging, message board, Blogs, and Chat) policies and standards. • Verify that Management has established written policies and procedures to supervise the activities, including electronic communications, of all required employees to achieve compliance with all applicable regulations. • Determine if the written policies and procedures include a list of all permitted forms of electronic communications to be used by employees and prohibit the use of all other platforms. • Verify that written policies include procedures and details for electronic communications archival and retention. • Determine how policies, standards, procedures, and regulations are communicated to employees and consultants and that management or ensures compliance. • Review e-mail policy; specifically, it should be in place and kept up to date relative to regulatory requirements and technology infrastructure. • Determine if the environment and procedures surrounding the use of third party applications (e-mail archiving system) are in compliance. Inquire if other subsidiaries of the firm are part of this environment and therefore should be included as part of the audit or if they have a separate process.

Risk To Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		• Verify that the policies and procedures address regulatory compliance as it pertains to retention, media storage, security and availability of electronic communications both nationally and globally.
D. Compliance		
Management is unaware of or does not fully understand regulatory requirements regarding electronic communications possibly leading to compliance issues or that regulatory requirements have not been clearly defined and documented by management possibly leading to compliance issues. Management does not have ability to demonstrate or prove to regulators that it is in compliance with electronic communications supervision requirements. Message reviewers and supervisors do not fully understand their	Compliance group has been established to understand, interpret and monitor all established and emerging regulatory requirements and concerns. Automated oversight and review procedures have been implemented and can be made available to regulators upon request. Evidence of review can be satisfied by use of a log or other record from the electronic communication compliance system that identifies the reviewers. Established training programs for electronic communications supervision teams that	• Determine if the firm's compliance group is aware of the regulatory issues related to electronic communication. • Measure the firm's compliance with the policies, standards, procedures, and regulations obtained above by testing certain controls in the standard against the firm's actual system settings. • Review the methods used to comply with the regulatory requirements. Understand the following: – Messages (original and duplicate) needs to be preserved exclusively; – Non-rewritable, non-erasable formats; – Able to verify automatically the accuracy of the archiving process; – Original and duplicate messages must be fully indexed and searchable; and – Messages must be maintained for 3 years, the first 2 of which must be in a readily available location. • Identify approved electronic communication services and ensure that only approved software is installed and in use. • Determine whether a procedure exists for the review of e-mails and if so review the following:

Risk To Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
responsibilities in regards to electronic communications supervision.	clearly communicate all regulatory requirements, company policies and electronic communications supervisory and automated procedures.	– Verify that the procedures clearly identify the person(s) responsible for performing the reviews and that they are performed within established reasonable frequencies and timeframes based on the type of business that is conducted; – Are there guidelines specifying who can examine e-mails (processing details or content) and under which circumstances? – Determine who has access to user's mailboxes and assess the access levels to ensure only authorized user have such access; – Ensure that a process is in place to record all access to user's mailboxes along with appropriate justification; and – Determine if there is a report on authorized/unauthorized users accessing another user's mailbox. • Ascertain if encryption of e-mails takes place (e.g., PGP) that those e-mails enter the archival area as unencrypted or can be unencrypted through a key provided to Compliance/Legal (otherwise can not be monitored or turned over for discovery). • Verify that the settings of specific policies for any automated oversight and review systems such as Live Communication Server (LCS) match those published in the written policies, standards, and procedures. • Review the output, logs, and alerts of the automated oversight and review system to ensure consistency with the settings and the written policies, standards, and procedures and those relevant copies are sent to the compliance group and management. • Verify that when members of restricted business group attempts to communicate in a prohibited manner, a copy of the communications attempt is sent to the relevant compliance groups and management.

Risk To Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		• Review process where appropriate for inbound and outbound e-mails to be reviewed by a third party • Review procedures for providing copies of messages, review logs, and other compliance reports to law enforcement and regulatory agencies. • Review electronic communication awareness programs; they should be in place and be repeated regularly for existing employees and communicated to all new employees at orientation. • Verify that all external mails contain a legal/compliance department approved disclaimer. • Determine if there is any business or department specific addendums to e-mails and verify that they too have been approved by legal/compliance. • Verify that the firm's network (i.e., e-mail server name, exchange version, send mail version, and internal IP) information is suppressed by sending a test mail to an external mail account. • Interview management responsible for electronic communication infrastructure about their knowledge of existing policies and standards. • Interview management to determine whether gaps in implementing policies are known and whether there is a plan to achieve compliance.

Risk To Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
E. System Architecture and Configuration		
Insufficient messaging server configurations can be exploited to gain privileged access to compromise e-mail security and integrity	Through inquiry and observation gain an understanding of the electronic communication system architecture and configurations: • Number and type of servers that support Electronic Messaging (e.g., Dev. Test and Prod, tools/admin, utilities, restore, archiving, and storage) • Number and variety of electronic messaging clients that exist in the production environment (i.e. Outlook, UNIX mail, and Outlook Web Access) • Number of mailboxes/ user accounts on each platform	• Conduct walkthrough meetings in order to develop an understanding of the electronic communications environment. • Obtain and evaluate the complete inventory listing of servers providing electronic communication applications that exist in the production and contingency environments. • Obtain technical documentation from administrators or system architects, including architecture diagrams and identify controls for evaluating message routing topology. • Obtain a full understanding of the roles that the electronic communication servers are performing and mailbox configurations through interviews and studying technical documentation from the step above, and assess how they are configured and controlled. – Are mailboxes appropriately sized? The message size limit is set at server level; – Determine whether there is a procedure for sending large mail. Verify that the handling of large mail is consistent with policies and procedures; – Are there public folder servers? If so, what is their associated support structure and whether there are any reliability issues? – Are Connector servers configured for proper isolation and ease of troubleshooting for messaging connectivity? – Are the front-end servers properly configured from a security standpoint? and – Determine if redundancy is built in so that data does not exist on a single failure point. • Verify all server configuration protocols to ensure that only

Risk To Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		approved and required protocols are installed and protected (i.e., SMTP, MAPI, RPC, x400, NNTP, POP3, and LDAP). • Review the electronic communication database architecture, if applicable, and determine whether the organization of storage groups and their associated databases is consistent with polices and procedures. • Obtain and review the settings of SMTP virtual server parameters to assess whether inbound message flow is properly controlled. • Engage the assistance of various administrators, Information Security analysts, and firewall administrators to locate non-standard e-mail systems and assess their impact on the security of Company's e-mail system architecture. • Identify the current installed version of the electronic communication server/client Software packages (i.e., e-mail, UNIX Mail, Microsoft, Blackberry, Outlook Web Access, and Chat). – Ascertain whether adequate documentation exists for server settings and security; – Obtain and identify the software versions, releases and service packs that should implemented; and – Verify the procedure for keeping software updated with current patches. • Obtain documentation system configuration for Internet Mail Gateway. – Determine whether the configuration is adequate; and – Verify that the Internet Mail Gateway only accepts and forwards authorized messages.

Risk To Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		• Obtain the e/mail routing configuration, e.g., routing rules. – Verify that authorized e-mail is configured to route to a proper destination; and – Inquire and assess the monitor procedure to ensure that e-mail is adequately routed. • Determine if controls have been put in place so that all production e-mail servers comply with the required process of filtering, collection and archival of e-mail communications. • Review the capability of the applications in place to respond to regulators request to obtain electronic communications for discovery purposes. • Review e-mail system Capacity; specifically, the e-mail system must have the capacity at all times to keep a full 2 years of e-mails in a readily accessible manner. • Electronic messaging storage media should enable compliance with regulatory requirements. Electronic storage media should be non-erasable (i.e., WORM disk). • Review the controls that have been put in place so that all production e-mail servers may comply with the established standards which have been implemented to promote consistency of messaging servers. • Select a sample of electronic messaging servers (to be determined in conjunction with the IT Audit Director) and compare their configuration to the secure server configuration prescribed by IT policies and procedures.

Risk To Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		• Verify that the settings for any encryption algorithms are in accordance with the firm's IT security policy. • Verify Instant Messaging client installation configurations for consistency with pre-established standards. – Determine the installation procedure for IM/Chat software and verify whether the configurations are appropriate and in compliance with policy; – Verify that unauthorized IM screen names are restricted from logging onto the firm's network; and – Determine and verify that the ability to manage file transfer, collaboration (e.g., audio/video conferencing), and other client privileges via instant messaging applications at the company, group, and individual employee levels are compliant with the firm's communication policy. • Determine if there are alarming mechanisms when messages are not captured due to capacity issues, the archival system has a backlog, or an index that becomes corrupted from a hardware failure. • Determine if the firm allows for remote e-mail services such as the Blackberry Enterprise Server and verify the following; – Verify that installation documentation exists; – Verify that e-mails send via remote e-mail services are archived; – Review device inventories and determine how many version of software exist, which versions support which devices, and whether all are on IT approved lists; – Determine if there any exception to the production version of remote e-mail services and verify that the need for such has

Risk To Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		been documented and approved; – Verify that policy configurations have been defined according to policies and procedures for the following: □ Default – Password Policy Group □ Security Policy Group □ Global Items □ Common Policy Group – Verify that password parameters are set in accordance to the firm's password policy. • Determine if the firm allows Short Message Service ("SMS") text messaging via the e-mail server or remote mail services such as Blackberry and verify the following; – Messages sent via SMS should be retained in accordance to the firm record retention policy; – Obtain the list of users that are SMS enabled and verify that appropriate approvals have been obtained for a sampling of users; and – For non-authorized SMS users, verify that their setting for SMS is disabled. • Determine if the firm allows pin-to-pin messaging via the email server or remote mail services such as Blackberry and verify the following; – E-mail sent via pin-to-pin method should be retained in accordance to the firm record retention policy; – Obtain the list of users that have pin-to-pin enabled and verify that appropriate approved for a sample of users; and – For non-authorized pin-to-pin users, verify that their setting for pin-to-pin is disabled.

Risk To Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		• Determine if the firm disallows electronic communication via the internet and if so review the following; – Verify that proxy settings do not allow access to e-mail/chat/IM web sites (generally these communications can not be monitored or archived); – Verify the control/configuration for blocking employees from using text messaging via the internet is set properly; – Verify that the control/configuration for preventing employees from accessing e-mail via the internet is set properly; and. – Verify that the control/configuration to prevent employees from using IM and Chat via the internet is set properly.
F. System Administration		
Lack of controls around system access and use by unauthorized users could cause disruptions, creation of unwanted messages, or the placing of malicious software within the electronic communication infrastructure. Restricted business groups (e.g., research and investment banking) that may utilize electronic communications methods to share information in violation of regulatory	The firm has assigned qualified personnel to perform supervision over employee electronic communications and to report on any activity that are potentially policy or regulatory violations. The firm has implemented a system to supervise the activities, including electronic communications of all required employees to achieve compliance with all applicable regulations.	• Review how the e-mail system is being administered. Determine the number of administrators of the e-mail system that have access to read all e-mail accounts. Is the number appropriate? Could they perform their job responsibilities with lower levels of access? • Review established user profiles and mailbox access rules for administrative users to ensure compliance with company policies and regulatory obligations. • Review the electronic messaging user administration process; account request, authorization, setup and termination process and Special requests (e.g., IM and Bloomberg) to ensure that only privileged users have access and that all activity is monitored and logged. • Determine if an automated supervision system exists that allows for the following;

Risk To Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
rules and business firewalls.	Controls that are designed to prevent or restrict communications between regulated business groups are tested to ensure that they are working as expected.	– Scanning of messages against pre-determined policies and has the ability to flag potential policy violations to system administrators; – Flagging of electronic communications that may evidence or contain customer complaints, problems, errors, orders or other instructions for an account; or evidence of conduct inconsistent with FINRA rules, federal securities laws and other matters of importance; – Message reviews by designated supervision team as well as ability to record, report and audit these manual review activities; and – Supervision system allows for the ability to record, report and audit all electronic communications supervision activities performed. • Determine the parties responsible for administering backup jobs and recovering storage group/databases from backups. Obtain their procedures and review for adequacy. • Obtain a list of e-mail system accounts, which likely maps to the Active Directory user list. Determine whether accounts exist for users no longer with the firm (e.g., reconcile against an HR list). • Determine if security settings are configured and maintained from a central location. • Review procedures for creating and granting permission for public folders. – Verify that access privileges to public folders are adequately controlled; – Determine if all public folders should have a designated owner;

Risk To Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		– Review procedures to ensure that access to public folders is assigned on a needs basis. Access to public folders should be assigned only with the approval of the owner; and – Verify that access permissions to critical or sensitive public folders are reviewed by owner on a regular basis. • Verify that no generic electronic communication accounts are created without the permission of Information Security and the head of the requesting department. • Review the electronic communication user administration process and account setup process for external mail providers such as Bloomberg to ensure that they conform to the firm's policy and procedures.
G. System Security		
Unauthorized access and use of the electronic communication services from the internet could create reputational risk to the firm. Viruses or other malicious content may infect the firm through e-mail. A virus could cause disruption of service and/or loss of data. The lack of filtering 'spamming' e-mail may	The use of firewalls and proxies to control inbound and outbound messages and attachments from the internet. Virus scanning software that detects and removes viruses in a timely manner from all forms of electronic communication including all attachments. Procedures and software to block e-mail spamming	• Verify that all electronic communication system components are protected from the Internet by a firewall and a proxy and review the following; – Firewall and proxy settings comply with the firm's policies and procedures; – Verify that the firewall been locked down to only allow the mail gateway to open a connection through to the internal network on an authorized port and that no other DMZ hosts are allow through the same port; and – Verify that proxy settings and access to proxy servers are password protected. • Verify that security settings over the e-mail, IM, and any chat/fax servers do not allow public access (which would expose these communications to modifications, leakage/unauthorized access).

Risk To Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
lead to degradations in server performance. Lack of controls to limit privileged access to the Electronic Messaging systems can lead to granting of unauthorized access and entitlements. Lack of controls to manage electronic messaging systems against IT Security Policy can result in unauthorized, illegitimate usage to non-firm approved messaging and chat that will not be captured, surveilled, archived, or blocked resulting in possible breach of information barriers.	from the Internet. Controlled access and log files to track activity that has occurred. Controls to ensure compliance with the firm's electronic communication policy. Electronic communications reviewers and supervisors are restricted to only employee messages for who they are authorized to review. Logical access controls based on cost center, employee IDs or departments are built into the supervisory system	• Determine if there is a procedure for monitoring for viruses and other malicious software? If yes, obtain and assess whether the procedure adequately addresses the following; – Verify that all incoming messages and attachments are filtered for viruses, potentially unwanted URL links, known SPAM domains, and inappropriate language or content; – Verify that all outgoing messages and attachments are filtered for viruses and inappropriate content; – Determine if filtering rules are used to restrict both individual source addresses and known SPAM domains in the FROM field of messages; – Verify that allowable instant messages and MS text messages are being scanned for inappropriate contents as well as executable attachments and attachments deemed unsafe. – Verify that IM rules do not allow the users to expand their capabilities (e.g., add external "buddies", internal front office or Investment banking personnel); – Determine how potentially dangerous attachments are removed, explanations provided to the recipient, and the process by which safe attachments can be retrieved; – Verify that the anti-virus administrator tests and updates virus definitions no later than 5 days from the most current vendor release date; and – Determine if the electronic communication infrastructure is vulnerable to viruses, worms if the archival system saves an attachment with a virus. • Determine if there is a procedure for monitoring and cleansing e-mail viruses? If yes, obtain and assess whether the procedure adequately addresses the necessary steps, including:

Risk To Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		– Escalation procedures; – Virus communication procedures; – Deployment of new hot fixes and virus definition file; and – Check that adequate procedures exist for regular virus scans on all servers. • Review network security and access over servers, folders and key data files to ensure that they are appropriately secured and privileged access to e-mails is controlled. • Review access to the third party data capture, surveillance, and compliance applications. Confirm that access is restricted to authorized personnel and verify that they cannot be disabled or bypassed. • Review the security around the transfer and collection of messages from third party electronic communications providers such as Bloomberg to ensure that they meet all the same requirements as other forms of electronic communication. • Determine if IT has a process to identify the use of unauthorized electronic communication applications, and select a sample to test their process. • Review documentation for anti-virus management in the e-mail system and obtain/review reports generated from the system. Determine the number of anti-virus incidents the system corrected vs. viruses that the system did not catch. • Verify that security patches for the electronic communication servers are tested and fully implemented during the next available

Risk To Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		configuration change cycle after the vendor's official release date, with the exception that emergency patches deemed high risk by system administrators are tested and applied immediately. • Verify that external parties, such as outside customers, contractors, and vendors do not have the ability to search for company contacts through searches of the electronic communication servers. • Determine the physical security controls over backup media including retrieval of archived data. Tour the storage facility and observe the storage of tapes onsite and the tapes being sent offsite. • Determine if administrators that configure the operating system have access to the messaging server, firewall, or proxy configurations. There should be a clear separation of responsibilities. • Determine what component of the configuration allows console access to take the system out of compliance mode and verify that only authorized users have access to it. Verify how many times the system been taken out of compliance since its installation through a report and determine if there have been legitimate and authorized reasons to do so. • Verify if monitors and/or alarms are raised if the electronic communication system becomes corrupt or has an integrity error with a digital signature, signs of potential external unauthorized intrusions. • Obtain the IP range for archival system and determine if the archival system address range is being scanned by Information Security and

Risk To Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		analyze for security weaknesses. • Determine if electronic faxes are in use and, if so, they meet the same requirements (e.g., non-erasable media). • Verify that new equipment (e.g., copiers) do not have e-mail capability and, if so, appropriate safeguards are in place (user must authenticate, e-mail can not be sent without being archived).
H. System Monitoring		
Lack of oversight and monitoring of the electronic communications infrastructure could allow system access and use by unauthorized users that could cause disruptions, creation of unwanted messages, or the placing of malicious software. Lack of oversight and monitoring of system variables such as capacity, message retention, throughput, etc could adversely affect the ability to process messages and create compliance issues.	Management should have a formal and documented procedure in place to continuously monitor the health, security, and activities of the various internal components of electronic communication and messaging services which addresses: • Availability; • Security' • Performance; and • Analysis/early warning on usage of electronic communication services.	• Verify that system, application and security logs are enabled for all electronic communication servers at all times and verify the following; – Verify that the minimum log size has been set to allow for sufficient logging of key security information with a minimum retention period as set by the firm for investigative purposes; – Verify that administrators provide reports for high usage to Information Security on a monthly basis or upon request from Information Security including inbound versus outbound statistics for message flow; – Verify that all appropriate hosts are monitored; and – Determine if logs are reviewed timely by qualified personnel? • Identify and assess the parameters currently being monitored by Exchange monitor and whether it covers: – Outgoing Queue (i.e., undeliverable mails and large mails in defer queue); – Incoming Queue (i.e., dead letters); – Average message delivery (i.e., urgent and non-urgent); – Latency with in acceptable time; – Alert IT when mails are sitting Queues for, say, one hr; and

Risk To Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		– Mailbox/Disk capacity. • Verify that electronic communication server performance and availability logs and reports exist and are reviewed on a timely and periodic basis. • Review controls that have been put in place to facilitate the generation and retention of adequate audit trails and verify the following; – Verify that audit trails are created for all forms of electronic communication (e-mail, instant messaging, IRC chat, and fax transmission); – Determine if audit trails of all modifications by authorized or unauthorized users are generated and retained; – Verify that audit trails cannot be modified by unauthorized users; – Determine if periodic reviews of audit trails are performed to identify unauthorized access; and – Determine if Unix to Unix communications are monitored and appropriate audit trails are generated. • Review Logical Access and Audit Logs – Determine the grouping of accounts (e.g., per user, per individual repository, and special purpose accounts); – Pull a list of groups and associated ACLS (Domain to repository) and track them back to the logs; – Pull logical access list of all groups within the system and determine if they meet job responsibilities; – Determine if reports can be written from the logs to identify what special purpose groups have been set up and their writes and the functions they have been performed (queries);

Risk To Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		– What are the archival system logs trapping and who is reviewing the logs? – How audit logs are setup (queries, retrievals, administrative operations) in the system and who reviews the logs and activity (should probably be info sys)? and – What is the mechanism to ensure the logs are not manipulated – log security on the application level as well as on the OS level? Decide if logical access for a database is also required. • Determine whether automated monitoring software is used and configured to perform any actions. If so, If there are more than one server is set up for monitoring [link monitor], confirm only one server is configured to carry out any given remedial action. • Verify that appropriate escalation procedures are in place based on action required as the result of monitoring. • Determine that log files are properly protected, as they are needed for recovery. Verify that all storage groups that house mailbox databases have circular logging disabled.
I. System Operation and Support		
Problems that are not identified and addressed in a timely manner could result in a reduction in user productivity. Inefficient and ineffective	A clearly defined and documented change control process so that, unauthorized changes cannot be migrated to production.	• Review controls that have been put in place so that scheduled maintenance and emergency changes do not negatively impact the availability of the electronic messaging system. • Review procedures for performing software upgrades. For major changes (i.e., system upgrades, functional enhancements) perform the following: – Determine the level of QA testing performed (including stress

Risk To Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
problem management due to a lack of controls. Long unavailability of IT services due to delay of solving problems.	• Change Management procedure should address the following areas: Submitting requests; Prioritization; • Version control; • Approvals; • Testing; • Emergency procedures; Roll-out procedure; Production migration; and Back out procedures. A formal and documented Problem Management procedure in place which addresses: • Submitting problem tickets; • Identifying the root cause of system problems. • Escalation procedures; • Approvals; • Reporting procedures; • Problem review procedures to address root causes; • Troubleshooting	testing); – Verify the existence of a test plan; and – Determine who signs off on the changes and to what extent the business is involved. • Review the messaging software emergency change control procedures (i.e. patching and bug fixes). • Review policies and procedures for performing mass data changes including mailbox restores and migrations. • Obtain relevant documentation, a sample list of change request, and interview electronic communication services support personnel to verify the following; – Management tracks the status of requests; – Details of the problem are documented; and – Determine if there is a system related root cause deficiency causing the problems.

Risk To Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
	procedures; and • Updating appropriate documentation.	
J. Business Continuity		
Lack of documented procedures for electronic communication Business Continuity can lead to non-standard, incomplete, or inaccurate messages and an inability for the firm to conduct critical operations in a timely manner. The lack of a formal backup and recovery process increases the risk of delays in system recovery.	Ability to facilitate electronic communication on a 24 x 7 basis. Backup procedures that conform to local standards and legal requirements.	• Determine if there is a written electronic communication BCP policy that clearly defines the need and importance of restoring and resuming electronic communication operations in the event of a disaster. • Determine if electronic communication recovery is covered in both the firm's overall BCP as well the firm's data center or third party service provider's BCP. • Obtain a copy of the business continuity plan and confirm that it caters for scenarios resulting in partial or total loss of supported systems, services and facilities. • Review the controls that have been put in place to facilitate timely system recovery in the event of a system failure and that if a system failure occurs, compliance with regulatory rules are maintained • Review the IT e-mail recovery policies and procedures. • Review backup procedures to determine whether they are adequate to meet both the firm's needs and to satisfy regulatory requirements. • Verify that at least one disaster recovery server is being kept available at all times and that a complete disaster recovery kit has been built and stored in a readily accessible location? • Review the e-mail trouble logs for the last ninety days to detect

Risk To Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		whether there have been any system failures within the recent past and how they were resolved versus the service level agreement. • Verify and test that an e-mail router contingency environment is exists. • Determine whether formal backup and recovery procedures exist for e-mail system, if yes, are they up to date. • Verify if IT has a restore procedure; verify that all requirements for e-mail restoration are available and accessible to IT. Has the restore procedure been tested? Determine how often a recovery test is performed. Obtain the test plan and test results. • Determine the procedure for storage of backup media and verify the following; – When and how often are backup tapes are sent offsite; – Is there exists a central group responsible for sending backup tapes offsite; – If a process exists for recalling backups when required; – That all data, software and documentation needed in disaster scenarios are readily available; and – The rotation method used for backups.
K. Archival, Retention and Retrieval		
Inbound and outbound electronic communications must be captured, archived, retained and blocked according to SEC retention and retrieval requirements;	Controls that have been put in place to facilitate compliance with the SEC electronic communication retention and retrieval requirements.	• Verify that the e-mail retention process and methodology are consistent with regulatory compliance and the firm's electronic communication policies and procedures as they pertain to archival and retrieval of stored messages. • Determine if the archival and backup processes of data from the

Risk To Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
otherwise the firm can be subject to violations. Messages are not readily available for retrieval requests as required by regulations. Retrieval requests are not processed timely (e.g., within 30 days) possibly resulting in regulatory fines.	Automated system controls ensure that all archived EC messages are indexed and easily searchable (e.g., by sender, receiver, date, and key words) to meet retrieval requests. Management has established a team responsible for coordinating responses to arbitration, litigation, and regulatory discovery cases including retrieving electronic communication for specified date ranges and named individuals when required. Controls to ensure that out of scope messages are not archived unnecessarily leading to additional storage costs.	electronic communications systems are timely and accurate including message contents, attachments, and meta data. • Review controls that have been put in place to comply with SEC e-mail retention and retrieval requirements. All business related communications should be retained as per applicable regulations. For the first two years all records should be maintained on readily accessible media, indexed and easily reproduced in a timely manner • Review configurations to verify that all mail boxes have copies kept where appropriate and list exceptions (if any). • Verify that fax and scan for e-mail are also forward for retention and surveillance. • Confirm that e-mail sent by Unix servers are also captured and retained. • Confirm that all e-mail sent through third party networks such as Bloomberg are also captured and retained. • Verify that a request process for electronic communications retrieval includes request review, approval and routing to the appropriate support group for fulfillment. • Verify that all IM conversations are recorded, archived, and monitored as per the firm's electronic retention policies and in accordance to regulatory requirements. • Obtain the architecture diagrams for the archival system integration with Mail, IM, and Chat servers and interview the Technical Services team to understand how they maintain a level of

Risk To Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		confidence that all traffic is captured by the archival system • Verify that the archival system configuration that determines the length of time e-mail, chat, and IM will be retained is appropriate. – Determine whether electronic messages retention requirements have been documented and are in compliance with Firm policy (e.g., 3, 5 year, or infinite). – Determine whether the Firm has policies and standards for purging electronic messages after the required retention period. – If the Firm has purging / destruction policies and standards, determine the process (i.e., identifying what type of electronic communications is included and excluded (e.g., litigation holds, tax data) from purging; frequency and method of purging data) for purging electronic messages. • Select a sample of active e-mail/Chat/IM users and mailboxes across geographic regions and various servers and verify that messages are stored in the archival system review repository. • Determine if consultants and sub-contractor electronic communications are also saved. • Determine that there is a backup/duplicate copy of the original available at all times. • Verify that storage formats that are non-rewritable and non-erasable. • Determine what auditing system are in place and the following audit capabilities exists: – How does the system audit changes made to the original and duplicate copies;

Risk To Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		– Can we make the auditing system available to external parties (e.g., staff of Commission); – Determine that the auditing logs are maintained for 3 years; and – Determine that the auditing capabilities are preserved (e.g., if in WORM media). • Determine who the third party is that has access to the firm's electronic communication infrastructure in order to provide information independently to the SEC if requested and how they get access. – How is this access monitored? – What is the procedure for the SEC to request information from Company regarding an investigation? – Who is the first point of contact technology/business? – What is the protocol for allowing the technology people granting access? and – Who is permitted to get access to another persons account? • Confirm that the archival system is always accessible and readable per Rule 17a-4 - At all times have available, for examination by the staffs of the Commission and self-regulatory organizations of which it is a member, facilities for immediate, easily readable projection or production of micrographic media or electronic storage media images and for producing easily readable images. • Determine if bgical access controls over the message archive and supporting infrastructure are in place to restrict access to only authorized personnel. • Determine how the archival system meets the following criteria:

Risk To Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		– Preserve the records exclusively in a non-rewriteable, non-erasable format; – Verify automatically the quality and accuracy of the storage media recording process; – Serialize the original and, if applicable, duplicate units of storage media, and time-date for the required period of retention the information placed on such electronic storage media; and – Have the capacity to readily download indexes and records preserved on the electronic storage media to any medium acceptable under this paragraph (f) as required by the Commission or the self-regulatory organizations of which the member, broker, or dealer is a member. • Determine the integrity of attachments are intact and that e-mail and IM that are deleted are still saved in the archival system • Pull of sample of e-mails containing attachments and determine that the following file attachments can be retrieved in readable form: Doc, PDF, Excel, PPT, and JPG. • Determine if the firm's Compliance area sent a notification letter to the examining authority notifying them that the archival system is in use. • Determine if automated system controls ensure that all electronic communications as defined by regulatory rules (e.g., e-mail, instant messages, and chat rooms) are archived and stored in a data repository. • Determine if automated system controls ensure that all archived messages are indexed according to relevant message meta data (e.g.,

Risk To Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		sender, receiver, date, and key words). • Verify if automated system controls ensure that non-regulated or unnecessary messages (e.g., meeting invites and out of office responses) are either not archived or removed from the data store on regular basis. • Verify that technology support groups have established a testing methodology and procedures to help ensure that systems are performing message archiving as expected. • Verify that technology support groups perform testing over electronic communications archiving systems and infrastructure on regular basis to ensure automated system controls and message archiving continue to perform as expected. • Determine if monitoring controls over archiving including automated system alerts, message counters, volume metrics and trending analyses are in place to ensure message archiving is being performed as expected. • Determine if archived message data is backed up and copies are stored in separate off site locations. • Determine if the firm uses "deal sites" (e.g., Intralinks) and, if so, verify that communications are archived.
L. Review of Third Parties Providing Archival Services		
Third party archival services are not compliant with SEC retention and retrieval requirements.	Controls that have been put in place to review third party services and their compliance with the SEC	• Identify Third Parties Providing Archival Services. • Determine if a designated body within the data center or a Vendor Management Office is in place to exercise on-going oversight of the

Risk To Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
Messages are not readily available for retrieval requests as required by regulations. Retrieval requests are not processed timely (e.g., within 30 days) possibly resulting in regulatory fines.	electronic communication retention and retrieval requirements. Management has established a team responsible for oversight of third party vendors.	service providers and / or vendors. If so, determine what reports and tools are used to execute this oversight. • Determine whether a third party agreement exists – a third party is needed to satisfy those provisions of SEC Rule 17a-4 (all e-mails are retained in unalterable fashion and stored in a readily accessible manner), third parties' access should be secured, documented and tested on a regular basis. • Review controls over access to third party e-mail services (e.g., Bloomberg). • Determine that Third party e-mail services provided by market data vendors comply with records retention requirements. • Verify with third parties how the archival system product meets the technical requirements of regulatory and compliance rules.
M. Service Level Agreements and Contracts		
Failure to maintain up to date contracts, service level agreements, and licenses could result in hardware and/or software failures that adversely impacts a firm's ability to operate an electronic communication infrastructure.	Contracts and SLA's Exist between firms and their vendor, are reviewed by legal and compliance, and are signed by appropriate signatories. Contracts are current and detail responsibilities of each party and contain appropriate clauses regarding confidentiality	• Verify that a procedure is in place to ensure that vendor services meet business requirements, an appropriate request for proposal (RFP) and bidding process is in place, that contract are formalized and retained, and that a legal should review is performed prior to the contract signing.. • Determine that there are Service Level Agreements with performance and reporting standard. • Review a sample of the 3rd party data center contracts. Check that the contract includes, at a minimum, performance requirement, penalty clauses, right to audit clauses, confidentiality requirement etc.

Risk To Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
	and termination. Maintenance and support agreements and conditions are up to date and license requirements are adhered to.	• Review if the co-location vendors performances fall short of the expected SLA and that technology management escalate the matter as documented in the contract. • For each relationship with a third-party hardware/software provider, confirm a formal contract is in place. Contracts with third parties should include: – Formal management and legal approval; – Definition of services/spares to be provided; – Cost of services / "out of contract" items; – Quantifiable minimum service level; – Content and frequency of performance reporting; – Penalties for non-performance; – Problem resolution process; – Agreement modification/dissolution process; – Duration of contract and renewal/review procedures; and – Security requirements and non-disclosure guarantees. • Perform the steps below for the following contracts of equipments and software used by the electronic communication servers and Virus and Spam Filtering software; – Contracts are signed and current; – Check signatories are of appropriate level; – Verify that Legal/Compliance have approved contracts prepared by vendors; and – Check there are no licensing issues.
N. Message Content Supervision		
Failure to comply with applicable federal	Written policies and procedures to guide	• Verify the existence of written policies with respect to electronic communication message content.

Risk To Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
securities laws and self-regulatory organization (SRO) rules with respect to electronic communication content. Compliance failures may impact a member's ability to adequately supervise its business and manage the member firm's reputational, financial and litigation risk;	employees on the use and content of electronic communication for regulated business activities. Education and training activities to ensure awareness and understanding of policies regarding message content and reporting obligations. Automated or periodic manual reviews of electronic communication to ensure compliance.	• Review the written polices and procedures with respect to the following; – Ensure that they provide appropriate guidance concerning other applicable areas of concern (e.g., the use of confidential, proprietary and inside information; anti-money laundering issues; gifts and gratuities; private securities transactions; customer complaints; front-running; and rumor spreading); – Ensure that they provide procedures for handling customer complaints including escalation and reporting to regulatory bodies as appropriate; – Identify the types of correspondence that will be pre- or post-reviewed; – Identify the organizational position(s) responsible for conducting reviews of the different types of correspondence; – Address the implementation of, and compliance with, the member's procedures for reviewing public correspondence; and – Prohibit employees from the use of electronic communications unless such communications are subject to supervisory and review procedures developed by the firm. • Determine if there are automated systems to flag electronic communications that may evidence or contain customer complaints, problems, errors, orders or other instructions for an account; or evidence conduct inconsistent with FINRA rules, federal securities laws and other matters of importance. If such automated systems exist do they; – Provide alerts to appropriate staff to review such messages; – Provide audit reports for review by internal and external auditors; and

Risk To Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		– Provide a rules based approach that in addition to the minimum regulatory requirements the software also allows a firm to identify other business areas that warrant supervisory review. • Absent an automated system to flag electronic communication messages with questionable content determine if there is a manual procedure in place to periodically spot check various forms of electronic messages with respect to customer complaints or prohibited business communications. • Verify that the policies identify authorized personnel by roles and/or responsibilities that may inspect and monitor electronic communications. • Determine if reviewers have sufficient knowledge, experience and training to adequately perform their reviews and are aware of relevant regulatory requirements. • Determine that compliance and discovery processes meet regulatory requirements for timeliness (e.g., 15 days), and includes all communications from all sources (e.g., Bloomberg, chat, and IM). • Determine which departments are blocked from communicating with one another and ensure that these are covered in the policies and procedures, that systemic firewalls exist between such business units to prevent unauthorized communication, and finally that a monitoring process exists to flag violations. • Verify that a member's legal and compliance department are copied on communications between regulated departments (i.e., non-research and research departments concerning the content of a

Risk To Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		research report). • Verify the existence and effectiveness of training programs designed to educate employees to understand and comply with the firm's policies and procedures regarding electronic communication content. • Verify that management or compliance ensures that all regulatory requirements are adhered to by all employees, consultants, vendors, business stakeholders, and relevant support groups. • Determine if management and/or compliance periodically re-evaluate the effectiveness of the procedures for reviewing public correspondence and consider any necessary revisions.
O. Prior Audit Issues		
Prior and/or ongoing issues that impair a firm from operating a compliant and effective electronic communications infrastructure.	Review of prior issues, resolution, and meeting of previously established target dates.	• Obtain a copy of prior electronic communication audit issues that related to this review and perform issue follow-up to ensure that actions are adequately resolved. • Review past reports for outstanding issues or previous problems. Consider: – Regulatory reports of examination; – Internal and external audit reports, including SAS 70 reports; – Business continuity test results; and – Organization's overall risk assessment and profile. • Review management's response to issues raised since the last examination. Consider: – Adequacy and timing of corrective action; – Resolution of root causes rather than just specific issues; and

Risk To Be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		– Existence of any outstanding issues.
P. Conclusions and Action Plan		
Failure to address the electronic communication audit gaps that impair a firm from maintaining safe, secure, and reliable business communications that subsequently impair business operations, profitability, as well as place the firm in non-compliance with regulations.	Discuss corrective action and communicate findings with management and audit sponsors.	• Identify gaps in the electronic communication audit. • Determine actions needed to close gaps. • Assign responsibility to action items. • Determine target date for each action. • Ensure review of action items becomes part of next audit.

III. Glossary

III. GLOSSARY

The definitions in this section shall apply to the terms as used in the audit guidelines. Where terms are not defined in this section or within another chapter, they shall be defined using their ordinarily accepted meanings within the context in which they are used.

Attachment	A name given to a file that is sent with an e-mail, an e-mail attachment can be any type of file (e.g., documents, images, and zipped files/folders).
Archival System	The computer systems and software to identify, catalog, and store infrequently updated digital files for later retrieval. Storage mediums may include CD-ROM, DVD, digital tapes, and hard drives.
Chat	An electronic conversation between two parties conducted via computers, servers, and/or the internet. Once a chat has been initiated, either user can enter text by typing on the keyboard and the entered text will appear on the other user's monitor in the appropriate chat dialogue box.
Electronic Communication	Messages exchanged between two parties through the use of Microsoft Exchange, Microsoft Outlook Web Access, Instant Messaging, Online Chat, Unix mail, and third party vendor services such as Bloomberg Mail in electronic or digital form
E-mail	Electronic messages sent or received via e-mail servers or third party service providers, G-Mail, HotMail, etc.
Encryption	Encryption is a process which is applied to electronic messages or other important data, and alters it to make it humanly unreadable except by someone who knows how to decrypt it with the proper keys. The complexity of the algorithms used means that a strongly encrypted message might require thousands of years of processing by very fast computers to break the encryption.
Firewall	A firewall is a system that secures a network, shielding it from access by unauthorized users. Firewalls can be implemented using software, hardware or a combination of both. In addition to preventing unrestricted access into a network, a firewall can also restrict data from flowing out of a network.
FINRA	The Financial Industry Regulatory Authority (FINRA), is the largest non-governmental regulator for all securities firms doing business in the United States. FINRA oversees over 5,000 brokerage firms, about 172,000 branch offices and more than 676,000 registered securities representatives. Created in July 2007 through the consolidation of NASD and the member regulation, enforcement and arbitration functions of the New York Stock Exchange.

Instant Messaging	Instant messaging, often shortened to simply "IM" or "IMing," is the exchange of text messages through a a software application in real-time. Generally included in the IM software is the ability to easily see whether a chosen friend, co-worker or "buddy" is online and connected through the selected service. Instant messaging differs from ordinary e-mail in the immediacy of the message exchange and also makes a continued exchange simpler than sending e-mail back and forth. Most exchanges are text-only, though popular services now allow voice messaging, file sharing and even video chat when both users have appropriate hardware.
Mail	Used in this context to refer to e-mail messages.
Mailbox	A logical storage container or folder within an e-mail application such as Microsoft Outlook to store e-mail messages.
Message	The text, audio, or video content exchanged electronically between two users of electronic communication software (e.g., e-mail, Chat, or Instant Messaging).
Mitigation	Activities taken to reduce the severity or consequences of an emergency.
Pin-to-Pin Messaging	Sending electronic messages between two personal digital assistant (PDA) devices such as Blackberry or a Palm via a network. Each device is assigned a unique eight-digit number called a personal identification number (PIN). You can send electronic messages directly to a user's PIN rather than to the user's e-mail address.
Proxy Server	In an enterprise that uses the Internet, a proxy server is a server that acts as an intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control, and caching service. A proxy server is associated with or part of a gateway server that separates the enterprise network from the outside network and a firewall server that protects the enterprise network from outside intrusion.
Risk Assessment	Business processes and the business impact analysis assumptions are stress tested with various threat scenarios. The result is an assessment of the impact each may have on the organization's ability to continue to deliver its normal business services.
Stakeholder	Any individual, group, or organization that might affect, be affected by, or perceive itself to be affected by the emergency.
Standard	A document, the main text of which contains only mandatory provisions using the word “shall” to indicate requirements and which is in a form generally suitable for common reference by member firms.

Storage Media	The hardware components that write data to-and read data from-storage media, the physical components, or materials, on which data is stored. Magnetic or optical disks, tape and cartridges, diskettes, compact disks, hard drives are examples of storage media. In the context of this audit the medium must be non-rewritable, that is once written it cannot be written over, and non-erasable, that is once written it cannot be erased from the medium.
System	A functional unit, consisting of one or more computers and associated software, that uses common storage for all or part of a program and also for all or part of the data necessary for the execution of the program, executes user-written or user-designated programs, and performs user-designated data manipulation.
User	A person who uses or interfaces with a computer system or one or more of the programs (software) running on a computer system. In the context of this audit this refers to a person who uses electronic communication software.
Virus	A computer virus is a piece of software code that is secretly introduced into a system in order to corrupt it or destroy data. Often viruses are hidden in other programs, documents, or attachments to e-mail and Instant Messages and when opened, the virus is installed and executed on the host computer.