RIA WorkSpace

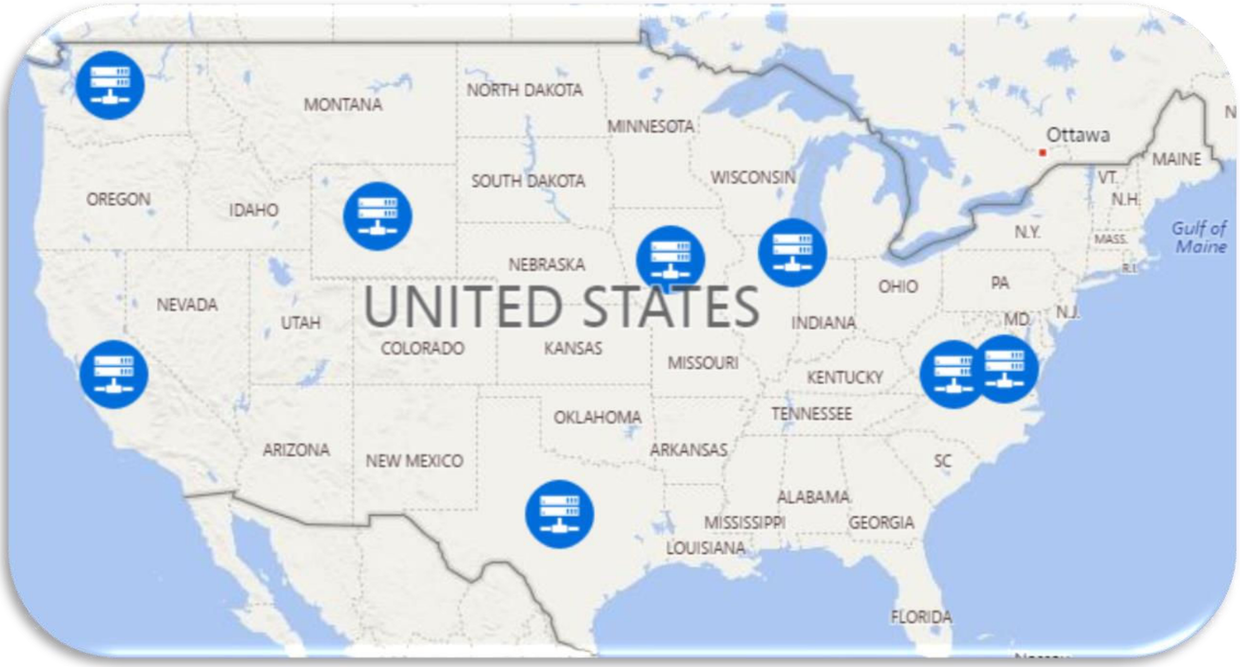
RIA WorkSpace with Advanced Security Technology Plan for [Company]

Contents

RIA WorkSpace

The RIA WorkSpace Platform in partnership with Microsoft Azure was designed to offer small and midsized financial services firm maximum flexibility without compromising security. An intuitive dashboard makes all your business files, data, and applications - both windows and web-based - accessible. A secure, centralized management system works to protect your data and make it easier for your business to comply with regulatory requirements.

National Data Center Footprint



Infrastructure Protection

RIA WorkSpace is a Microsoft partner and leverages azure infrastructure includes hardware, software, networks, administrative and operations staff, and the physical data centers that house it all. RIA WorkSpace addresses security risks across its infrastructure.

Physical security**.** This runs in geographically distributed Microsoft facilities, sharing space and utilities with other Microsoft Online Services. Each facility is designed to run 24x7x365 and employs various measures to help protect operations from power failure, physical intrusion, and network outages. These datacenters comply with industry standards (such as ISO 27001) for physical security and availability. They are managed, monitored, and administered by Microsoft operations personnel.

Fire Suppression**.** The Microsoft Azure fire protection approach includes the use of photoelectric smoke detectors installed below the floor and on the ceiling, which are integrated with the fire protection sprinkler system. Additionally, there are Xtralis VESDA (Very Early Smoke Detection Apparatus) systems in each colocation which monitor the air. VESDA units are highly sensitive air sampling systems installed throughout multiple high-value spaces. VESDA units allow for an investigative response prior to an actual fire detection alarm. 'Pull station' fire alarm boxes are installed throughout the datacenters for manual fire alarm notification. Fire extinguishers are located throughout the datacenters and are properly inspected, serviced, and tagged annually. The security staff patrols all building areas multiple times every shift. Datacenter personnel perform a daily site walk-through ensuring all fire watch requirements are being met. Areas containing sensitive electrical equipment (colocations, MDFs, etc.) are protected by double interlock pre-action (dry pipe) sprinkler systems. Dry pipe sprinklers are a two-stage pre-action system that requires both a sprinkler head activation (due to heat) as well as smoke detection to release water. The sprinkler head activation releases the air pressure in the pipes which allows the pipes to fill with water. Water is released when a smoke or heat detector is also activated. Fire detection/suppression and emergency lighting systems are wired into the datacenter UPS and generator systems providing for a redundant power source.

Redundant Power Systems. Redundant power includes uninterruptible power supplies (UPS) and backup generators, including on-site multiple-day fuel supply. Generator power is activated automatically in the event of a grid failure.

- Carrier diversity via multiple Tier 1 providers
- Redundant backup diesel generators, including on-site multiple-day fuel capacity.
- Redundant 208v/30amp power to each cabinet
- N+1 HVAC
- N+1 UPS
- N+1 generator
- N+1 power distribution unit (PDU)

Flood Control & Earthquake Management. All Azure Data Centers are above sea level, as well as 500-year flood plains. They have no basements, have tightly sealed conduits, and moisture barriers on the exterior walls. Every Azure Data Center contains dedicated pump rooms, drainage/evacuation systems, and moisture detection sensors. Azure Data Centers are built to meet or exceed seismic design requirements of local building codes for lateral seismic design forces.

Monitoring and logging. Centralized monitoring, correlation, and analysis systems manage the large amount of information generated by devices within the Azure environment, providing continuous visibility and timely alerts to the teams that manage the service. Additional monitoring, logging, and reporting capabilities provide visibility to customers.

Update management. Security update management helps protect systems from known vulnerabilities. Azure uses integrated deployment systems to manage the distribution and installation of security updates for Microsoft software. Azure uses a combination of Microsoft and third-party scanning tools to run OS, web application, and database scans of the Azure environment.

Antivirus and antimalware. Azure software components must go through a virus scan prior to deployment. Code is not moved to production without a clean and successful virus scan. In addition, Microsoft provides native antimalware on all Azure VMs. Microsoft recommends that customers run some form of antimalware or antivirus on all virtual machines (VMs). Customers can install Microsoft Antimalware for Cloud Services and Virtual Machines or another antivirus solution on VMs, and VMs can be routinely reimaged to clean out intrusions that may have gone undetected.

Penetration testing. Microsoft conducts regular penetration testing to improve Azure security controls and processes. Microsoft understands that security assessment is also an important part of our customers' application development and deployment. Therefore, Microsoft has established a policy for customers to carry out authorized penetration testing on their own—and only their own—applications hosted in Azure.

DDoS Protection. Azure has a defense system against Distributed Denial-of-Service (DDoS) attacks on Azure platform services. It uses standard detection and mitigation techniques. Azure's DDoS defense system is designed to withstand attacks generated from outside and inside the platform.

Network Protection

Azure networking provides the infrastructure necessary to securely connect VMs to one another and to connect on-premises data centers with Azure VMs. Because Azure's shared infrastructure hosts hundreds of millions of active VMs, protecting the security and confidentiality of network traffic is critical. In the traditional datacenter model, a company's IT organization controls networked systems, including physical access to networking equipment. In the cloud service model, the responsibilities for network protection and management are shared between the cloud provider and the customer. Customers do not have physical access, but they implement the logical equivalent within their cloud environment through tools such as Guest operating system (OS) firewalls, Virtual Network Gateway configuration, and Virtual Private Networks.

Network isolation. Azure is a multitenant service, meaning that multiple customers' deployments and VMs are stored on the same physical hardware. Azure uses logical isolation to segregate each customer's data from that of others. This provides the scale and economic benefits of multitenant services while rigorously preventing customers from accessing one another's data.

Virtual networks. A customer can assign multiple deployments within a subscription to a virtual network and allow those deployments to communicate with each other through private IP addresses. Each virtual network is isolated from other virtual networks.

VPN and Express Route. Microsoft enables connections from customer sites and remote workers to Azure Virtual Networks using Site-to-Site and Point-to-Site VPNs. For even better performance, customers can use an optional ExpressRoute, a private fiber link into Azure data centers that keeps their traffic off the Internet.

Encrypting communications. Built-in cryptographic technology enables customers to encrypt communications within and between deployments, between Azure regions, and from Azure to on-premises data centers.

Data Protection

Azure allows customers to encrypt data and manage keys, and safeguards customer data for applications, platform, system, and storage using three specific methods: encryption, segregation, and destruction.

Data isolation. Azure is a multitenant service, meaning that multiple customers' deployments and virtual machines are stored on the same physical hardware.

Protecting data at rest. Azure offers a wide range of encryption capabilities, giving customers the flexibility to choose the solution that best meets their needs. Azure Key Vault helps customers easily and cost effectively streamline key management and maintain control of keys used by cloud applications and services to encrypt data.

Protecting data in transit. For data in transit, customers can enable encryption for traffic between their own VMs and end users. Azure protects data in transit, such as between two virtual networks. Azure uses industry standard transport protocols such as TLS between devices and Microsoft datacenters, and within datacenters themselves.

Encryption. Customers can encrypt data in storage and in transit to align with best practices for protecting confidentiality and data integrity. For data in transit, Azure uses industry-standard transport protocols between devices and Microsoft datacenters and within datacenters themselves. You can enable encryption for traffic between your own virtual machines and end users.

Data destruction. When customers delete data or leave Azure, Microsoft follows strict standards for overwriting storage resources before reuse. As part of our agreements for cloud services such as Azure Storage, Azure VMs, and Azure Active Directory, we contractually commit to specific processes for the deletion of data.

Identity and Access

Enterprise cloud directory.
Azure Active Directory is a comprehensive identity and access management solution in the cloud. It combines core directory services, advanced identity governance, security, and application access management. Azure Active Directory makes it easy for developers to build policy-based identity management into their applications. Azure Active Directory Premium includes additional features to meet the advanced identity and access needs of enterprise organizations. Azure Active Directory enables a single identity management capability across on-premises, cloud, and mobile solutions.

Multi-Factor Authentication.
Microsoft Azure provides Multi-Factor Authentication (MFA). This helps safeguard access to data and applications and enables regulatory compliance while meeting user demand for a simple sign-in process for both on premises and cloud applications. It delivers strong authentication via a range of easy verification options—phone call, text message, or mobile app notification—allowing users to choose the method they prefer.

Access monitoring and logging.
Security reports are used to monitor access patterns and to proactively identify and mitigate potential threats. Microsoft administrative operations, including system access, are logged to provide an audit trail if unauthorized or accidental changes are made. Customers can turn on additional access monitoring functionality in Azure and use third-party monitoring tools to detect additional threats. Customers can request reports from Microsoft that provide information about user access to their environments.

Regulatory Compliance

Every Data Center is SSAE16 SOC1 Type II compliant, meets Securities and Exchange Commission (SEC) requirements, complies with the Sarbanes-Oxley (SOX) Act, and Health Insurance Portability and Accountability Act (HIPAA) guidelines.

Compliance Reports

All of the Compliance Reports for the platform can be found here.

You will be prompted to sign into your cloud resources to view all the compliance reports.

[Company] IT Narrative

[Company] has outsourced the Information Technology function to RIA WorkSpace in **Month** of **Year**. RIA WorkSpace is a professional services firm that proactively manages IT for companies. We take the worry out of managing your own IT and save you time and money. We want you to think of us as your own technology department. Our goal is to provide a predictable IT budget, reduce total cost of IT ownership and improve the reliability and performance of your IT systems. Only authorized employees of RIA WorkSpace have access to the computer servers and authorization to enable or disable network users. RIA WorkSpace monitors and manages the servers and desktop machines in the [Company] office, deploying patches and updates, as necessary. RIA WorkSpace can provide monthly monitoring reports, detailing the status of antivirus updates, space and memory usage and other information regarding network usage upon request.

Local Firewall

[Company] currently is running a **Manufacture Model** with the Comprehensive Gateway Security Suite. [Company] also has OpenDNS in place provided by RIA WorkSpace that delivers security at the DNS layer from the firewall, using the Internet's existing infrastructure, to keep malware from compromising their systems and to stop botnets or phishing from exfiltrating their data for additional application layer security. They also utilize Microsoft Defender for Endpoint that delivers security at the DNS layer from the endpoint, using the Internet's existing infrastructure, to keep malware from compromising their systems and to stop botnets or phishing from exfiltrating their data for additional application layer security.

Servers

Currently [Company] has **X** servers at the Data Center:

1. Server 1 (Server Role)
2. Server 2 (Server Role)

Anti – Virus Solution

[Company] utilizes Microsoft Windows 10 Defender and for Next Generation protection Microsoft Defender for Endpoint.

Email

[Company] Email resides on the Microsoft Office 365 Hosted Exchange Platform. They also utilize Global Relay for Journaling & Archiving for all inbound & outbound emails.

Advanced Security Technology

- [Company] utilizes the following additional security services:
    - Multifactor authentication, conditional and secure remote access to the RIA WorkSpace Platform for all their users.
    - Multifactor authentication, and conditional access for critical web-based apps.
    - Advance Threat Protection that includes.
        - Microsoft Defender for Endpoint
            - Microsoft Defender for Endpoint is a holistic, cloud delivered endpoint security solution that includes risk-based vulnerability management and assessment, attack surface reduction, behavioral based and cloud-powered next generation protection, endpoint detection and response (EDR), automatic investigation and remediation, managed hunting services, rich APIs, and unified security management.
        - Microsoft Defender for Office 365
            - Protect all of Office 365 against advanced threats like business email compromise and credential phishing. Automatically investigate and remediate attacks.
        - Microsoft Defender for Identity
            - Leverage real-time analytics and data intelligence with Microsoft Defender for Identity to prioritize and surface real threats. New detections are implemented and delivered directly from the cloud so [Company] can benefit from them as soon as possible.
    - Microsoft Cloud App Security is a Cloud Access Security Broker (CASB)
        - Supports various deployment modes including log collection, API connectors, and reverse proxy. It provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all [Company] Microsoft and third-party cloud services. The Cloud App Security framework consists of:
            - Discover and control the use of Shadow IT: Identify the cloud apps, IaaS, and PaaS services used by [Company]. Investigate usage patterns, assess the risk levels and business readiness of more than 16,000 SaaS apps against more than 80 risks. Start managing them to ensure security and compliance.
            - Protect your sensitive information anywhere in the cloud: Understand, classify, and protect the exposure of sensitive information at rest. Leverage out-of-the box policies and automated processes to apply controls in real-time across all [Company] cloud apps.
            - Protect against cyberthreats and anomalies: Detect unusual behavior across cloud apps to identify ransomware, compromised users, or rogue applications, analyze high-risk usage and remediate automatically to limit the risk to [Company].
            - Assess the compliance of your cloud apps: Assess if your cloud apps meet relevant compliance requirements including regulatory

compliance and industry standards. Prevent data leaks to non-compliant apps, and limit access to regulated data.

- Information Protection & Governance
    - Protect and govern data wherever it lives.
    - Protect your sensitive data throughout its lifecycle by applying sensitivity labels linked to protection actions like encryption, access restrictions, visual markings, and more.
    - Apply a consistent set of data loss prevention policies across the cloud, on-premises environments, and endpoints to monitor, prevent, and remediate risky activities with sensitive data.
    - Manage information lifecycle and records intelligently with in-place management, automated policies, defensible disposal, and pre-built data connectors.
- Insider Risk Management
    - Identify and remediate critical insider risks.
    - Detect, identify, and act on potential risks within [Company] with insider risk management.
    - Quickly identify and remediate code-of-conduct policy violations that occur across [Company] communications to support a healthy work environment and meet industry-specific compliance requirements.
    - Restrict communications among specific groups of users with help from information barriers.
    - Increase your control with explicit access authorization for service operations using customer lockbox.
    - Control privileged admin access based on specific tasks.
- Discover & Respond.
    - Quickly investigate and respond with relevant data.
    - Native eDiscovery capabilities for Teams, Yammer, SharePoint Online/OneDrive for Business, and Exchange Online simplifies the discovery and review of Office 365 content (e.g., Teams conversation reconstruction, edited Teams chat, support for linked content from OneDrive and SharePoint Online).
    - Machine learning and intelligent capabilities such as near duplicate detection, email threading, relevance, themes, and smart tags help customers to reduce and cull large volumes of data in-place to relevant set.
    - Access to audit events (e.g., the number of mail items accessed) that can help scope data that may have been compromised.
    - Advanced Audit helps [Company] to customize their audit log retention policy for up to a year to support their forensic investigations. To further help meet more rigorous regulatory, internal compliance obligations or conduct longer running investigations – organizations have the option to add-on the capability to retain their audit log activities for 10 years.

- Security Training Platform
    - Annual security training
    - Weekly micro-security training
        - Annual security training covers the basics while ongoing weekly micro-security training keeps [Company] users up-to-date and help [Company] fortify their human defenses.
    - Employee vulnerability assessments
        - The Employee Vulnerability Assessment takes the key security metrics and adds engagement with an interactive leaderboard and friendly competition.
    - Dark web monitoring
        - Ongoing dark web monitoring alerts [Company] the moment employee credentials show up on the dark web. Push password resets and stop a breach before it happens.
    - Simulated phishing campaigns
        - Phishing is the #1 attack method of choice among cybercriminals. Keep security top-of-mind with automated, simulated phishing campaigns sent to the [Company] team monthly.
    - Monthly security newsletter
        - Monthly security newsletter and personal dark web scanning capabilities allow [Company] employees to protect themselves at work and at home.
    - Security policy templates and portal
        - With written security policy templates and a policy acknowledgement portal, ensure [Company] employees know the proper procedures while tracking their annual agreements.

Backups

Where are the backups kept.

Microsoft 365 environment

Backup: There are two types of backup running

1. Site Level:
    a. This called Auto versioning. You can store, track, and restore items in a list and files. Versioning, combined with other settings, such as checkout, gives you a lot of control of the content that is posted on your site and can provide real value if you ever have a need to look at or restore an old version of an item or file.
    b. You can set unlimited versions that allows you restore files from previous years.
    c. Deleted versions will go to Recycle Bin.
2. Tenant Level:
    a. Microsoft backup every 12 hours and data kept for 14 days, and you can request a site to be restored.

What is Backed up:

The following locations are included:

- Exchange email
- OneDrive accounts
- SharePoint sites
- Office 365 groups
- Teams channel messages
- Teams chats

When is it backed up and how often:

There are several situations that generate backup:

- When a list item or file is first created or when a file is uploaded.
- When a file is uploaded that has the same name as an existing file.
- When the properties of a list item or file are changed.
- When an Office document is opened and saved. After a document is opened again, a new version will be created after an edit is saved.
- Periodically, when editing and saving Office documents. Not all edits and saves create new versions. When saving edits frequently, for example, each new version captures a point in time rather than each individual edit. This is common when autosave is enabled.
- During co-authoring of a document, when a different user begins working on the document or when a user clicks save to upload changes to the library.

How many versions of a document are kept:

- Keep the following number of major versions: 500 version.
- Retention Policy set at keep contents forever.

Archive:

Retention Policy set at keep content forever will follow two paths:

1. If the data is deleted or modified:
    a. Copy of the data will be placed on the Preservation Hold Library
    b. Timer job that runs periodically will identifies which files/folder retention period has expired.
    c. Files/Folders are permanently deleted within seven days at the end of the retention period.
2. If the data is not deleted or modified:
    a. Data will move to First Stage Recycle bin at the end of retention period.
    b. If the data empties from Recycle bin, Data moved to Second Stage Recycle bin
    c. After 93 days data will be permanently deleted

Due Diligence Report

General Information

Company Name	InhouseCIO LLC
Address:	8770 West Bryn Mawr Ave Suite 1300 Chicago, IL 60631
Telephone	877-361-3499
Website	www.inhousecio.com
Name and Title of Contact	David Kakish, President
Contact Telephone Number	773-530-1234
Contact Email	helpdesk@inhousecio.com
How many employees do we employ	19
Overview of InhouseCIO	InhouseCIO provides your company with an assigned team and proven IT processes so you can eliminate your IT headaches, have some peace of mind and keep your IT operations running smoothly and securely.
Services Provided to Clients	We provide managed IT & cloud services
Number of Years has been in business	Since 2007
Any changes to the Firms Owner structure in the past 3 years	None
Is the Company registered with any regulatory bodies?	We are registered the State of Illinois
Who is responsible for compliance in the Company?	Kal Heet
Are employees & contractors required to sign a Code of ethics, or any other agreement that obligate the employee or contractor to not disclose, and to preserve the confidentiality of, our confidential information as well as clients.	Yes, upon hire, and periodically thereafter.
Do you impose disciplinary measures for violations of company policies, including information security policies	Yes we do.

Insurance

InhouseCIO carries the following Insurance	• Professional and Technology E&O Liability • Media Liability • Network Security & Privacy Liability • Privacy Breach Expense

Business Continuity & Disaster Recovery

Does the Company have a formal disaster recovery plan?	Yes
What contingency plans does the Company have in terms of:	Data Breach Response Policy Disaster Recovery Plan Policy
How are clients notified of a Business Continuity & Disaster Recovery event?	Disaster Recovery Plan Policy

Cybersecurity & Information Security

Are procedures in place to protect against unauthorized access to the company's network and files	Yes
Has the company ever experienced a data breach? If so, describe the extent of the breach and any steps taken to avoid similar breaches in the future.	No
Does the company use 2nd Factor Authentication?	Yes – We use a Multifactor Authentication as well as single sign on.
Does the company conduct testing of the Cybersecurity program? If so, when was the last test?	Yes. This is performed on a Monthly basis

SEC OCIE Cybersecurity Initiative RIA WorkSpace Analysis

Executive Summary

The U.S. Securities and Exchange Commission's Office of Compliance Inspections and Examinations (OCIE) issues risk alerts on a regular basis. SEC regulated firms need to implement cybersecurity controls to protect customer data. These alerts were developed to provide guidance to registered broker-dealers (BD) and registered investment advisors (RIA) regarding assessment of their respective firms' cybersecurity preparedness. The Risk Alerts are not a request for any information to be provided to the SEC at this point in time.

Broker-dealers and registered investment advisors are required to protect customer information whether they outsource any of their IT function or maintain it "in-house". This analysis outlines controls SEC regulated firms should implement to protect customer information. Steps to be taken by each firm are noted, along with controls managed by RIA WorkSpace.

The data centers that RIA WorkSpace uses achieved SSAE 16 SOC 1 Type 2 certification that includes a description of management controls, control objectives, and the results of tests of control adequacy. Multiple control objectives relate to information security. No exceptions were identified by the service auditor.

Disclaimer

RIA WorkSpace is not directly subject to SEC regulation as RIA WorkSpace does not provide any investment services to, or directly interact with, consumers. The information included in this document is provided for current and prospective clients to gain an understanding of information security initiatives at RIA WorkSpace based on the SEC Risk Alert. RIA WorkSpace takes information security seriously. We protect client data as if it were our own. The information contained in this document is an overview of security initiatives and cannot be construed as being a full and complete description of all security activities. RIA WorkSpace retains the right to modify security initiatives at any time based on the changes in the risk assessment.

The OCIE states that they will be conducting examinations of more than 50 registered broker-dealers and registered investment advisors. Please note that this Risk Alert is not an actual request for information from any Broker/Dealer, RIA, or from RIA WorkSpace. Nor is this Risk Alert an indication that an examination will be conducted at any specific firm. Finally, the OCIE states:

"This document should not be considered all-inclusive of the information that OCIE may request. Accordingly, OCIE will alter its requests for information as it considers the specific circumstances presented by each firm's particular systems or information technology environment."

Cybersecurity Preparedness

An analysis of each control category and the sample information request list was performed by RIA WorkSpace. We identify policies, procedures, and controls that should be implemented by the BD / RIA firm. We also identify RIA WorkSpace policies, procedures, and practices in place to help protect each firm's information. Finally, we identify how we can help a firm create additional documentation or implement additional controls to help ensure appropriate data protection is in place.

Please note that the guidance outlined in this document is generic to BD / RIA firms and does not represent specific recommendations for any individual firm. Each firm needs to perform a risk assessment of their current control environment and determine if controls within the firm are adequate based on the firm's level of risk tolerance.

Identification of Risks/Cybersecurity Governance

1. For each of the following practices employed by the Firm for management of information security assets, please provide the month and year in which the noted action was last taken; the frequency with which such practices are conducted; the group with responsibility for conducting the practice; and, if not conducted firm wide, the areas that are included within the practice. Please also provide a copy of any relevant policies and procedures.

FIRM - Recommended Actions	RIA WORKSPACE
• Create an inventory of all IT assets (hardware and software) and develop a risk ranking. • Develop a basic network diagram.	• RIA WorkSpace maintains an IT asset inventory and network diagrams for all assets maintained within RIA WorkSpace. • RIA WorkSpace Cloud Desktop and server activity is logged along with sensitive activity on internal systems. External connections are monitored.

2. Please provide a copy of the Firm's written information security policy.

FIRM - Recommended Actions	RIA WORKSPACE
• Write an Information Security Policy (ISP) that includes: ○ Assignment of responsibility ○ Requirement for a risk assessment ○ Logical and physical access controls ○ Monitoring and testing of controls ○ Awareness training ○ Vendor management	• RIA WorkSpace maintains a comprehensive information security program, based on a written information security policy that includes: ○ Assignment of responsibility ○ Requirement for a risk assessment ○ Logical and physical access controls ○ Monitoring and testing of controls

3. Please indicate whether the Firm conducts periodic risk assessments to identify cybersecurity threats, vulnerabilities, and potential business consequences. If such assessments are conducted:

FIRM - Recommended Actions	RIA WORKSPACE
• Perform a risk assessment and identify any items deemed to be high or medium risk.	• RIA WorkSpace facilitates an annual risk assessment. Logical, physical, and service provider risks are assessed. • No items were noted with high or medium residual risk.

4. Please indicate whether the Firm conducts periodic risk assessments to identify physical security threats and vulnerabilities that may bear on cybersecurity. If such assessments are conducted:
   a. Same as response to #3.

5. If cybersecurity roles and responsibilities for the Firm's workforce and managers have been explicitly assigned and communicated, please provide written documentation of these roles and responsibilities. If no written documentation exists, please provide a brief description.

FIRM - Recommended Actions	RIA WORKSPACE
• Identify roles and responsibilities for cybersecurity in the Information Security Policy. ○ Designate a person as the Firm's "Information Security Officer". ○ Require all employees to protect client data and acknowledge responsibility for doing so. ○ Conduct regular security awareness training.	• Responsibility for cybersecurity is documented in the Information Security Policy. All employees are required to read and acknowledge compliance.

6. Please provide a copy of the Firm's written business continuity of operations plan that addresses mitigation of the effects of a cybersecurity incident and/or recovery from such an incident if one exists.

FIRM - Recommended Actions	RIA WORKSPACE
• Select a backup plan that is appropriate for your business. RIA WorkSpace provides multiple backup options. • Document a business continuity plan (BCP) -procedures to ensure all employees are safe and can get access to all the information needed to continue operations in the event of a disaster. Ideally, a BCP should be developed based on a business impact analysis (BIA) that identifies how when each business function needs to be available to support customers. The firm needs to consider how to work with customers and all service providers.	• The RIA WorkSpace business continuity strategy addresses points of failure within the organizational infrastructure and the deployment of recovery processes to provide business stability. However, RIA WorkSpace contingency strategies are solely intended for its own internal infrastructure and are not intended to replace any client-specific BC/DR plan or satisfy any BC/DR planning requirements. • Please refer to the "Business Continuity and Recovery Strategy Statement" for additional information.

7. Does the Firm have a Chief Information Security Officer or equivalent position? If so, please identify the person and title. If not, where does principal responsibility for overseeing cybersecurity reside within the Firm?

FIRM - Recommended Actions	RIA WORKSPACE
• Identify the person within the firm responsible for cybersecurity.	• RIA WorkSpace has designated the Chief Technology Officer as responsible for managing cybersecurity.

8. Does the Firm maintain insurance that specifically covers losses and expenses attributable to cybersecurity incidents? If so, please briefly describe the nature of the coverage and indicate whether the Firm has filed any claims, as well as the nature of the resolution of those claims.

FIRM - Recommended Actions	RIA WORKSPACE
• The firm should evaluate the need for errors and omissions and other cyber insurance.	• RIA WorkSpace maintains appropriate levels of insurance. No claims have been filed.

Protection of Firm Networks and Information

9. Please identify any published cybersecurity risk management process standards, such as those issued by the National Institute of Standards and Technology (NIST) or the International Organization for Standardization (ISO), the Firm has used to model its information security architecture and processes.

FIRM - Recommended Actions	RIA WORKSPACE
• Please refer to number 4 above.	• Please refer to number 4 above.

10. Please indicate which of the following practices and controls regarding the protection of its networks and information are utilized by the Firm and provide any relevant policies and procedures for each item.

FIRM - Recommended Actions	RIA WORKSPACE
• Document policies and practices related to cybersecurity to address each of the areas identified in the Risk Alert. • Establish appropriate controls, based on the risk assessment, for assets owned and managed by the firm. • Periodically test (audit) controls owned and managed by the firm.	• RIA WorkSpace has implemented many policies, practices and controls designed to protect networks and information based on our ISP. While specific controls are considered confidential to help protect the RIA WorkSpace services and platform, some of our controls include: ○ Security awareness training. ○ Assets are protected based on the concept of least privilege. ○ Separate test and production environments are maintained. ○ Asset management procedures exist. ○ Policies address removable media, malware, data storage, and data destruction. ○ Recovery from backup is tested.

11. Please indicate whether the Firm makes use of encryption. If so, what categories of data, communications, and devices are encrypted and under what circumstances?

FIRM - Recommended Actions	RIA WORKSPACE
• Document the use of encryption within the Firm. This may include encryption of hard drives or email.	• RIA WorkSpace has a documented encryption management policy and key management procedures exist. ○ Backups are encrypted. ○ Console connections are encrypted. ○ All access to the Cloud Desktop is encrypted using SSL.

12. Please indicate whether the Firm conducts periodic audits of compliance with its information security policies. If so, in what month and year was the most recent such audit completed, and by whom was it conducted?

FIRM - Recommended Actions	RIA WORKSPACE
• Periodically audit for compliance with the Firm's information security policy. • Consider auditing cybersecurity policies and systems configurations using the SEC Risk Alert as an audit guide.	• Independent SSAE 16 SOC 1 audits are conducted at the data centers. • Vulnerability scans are performed on a regular basis.

Risks Associated with Remote Customer Access and Funds Transfer Requests

13. Please indicate whether the Firm provides customers with on-line account access. If so, please provide the following information:

FIRM - Recommended Actions	RIA WORKSPACE
• If customers have online access, describe the services provided. A service provider brochure or customer information packet / customer sign-up packet may provide enough information. • Describe the service provider's security requirements and how your firm authenticates customers.	• Not Applicable.

14. Please provide a copy of the Firm's procedures for verifying the authenticity of email requests seeking to transfer customer funds. If no written procedures exist, please describe the process.

FIRM - Recommended Actions	RIA WORKSPACE
• Document procedures used to verify the authenticity of customer email requests.	• Not Applicable.

15. Please provide a copy of any Firm policies for addressing responsibility for losses associated with attacks or intrusions impacting customers.

FIRM - Recommended Actions	RIA WORKSPACE
• Describe any policies your firm or service provider has related to customer protection guarantees.	• Not Applicable.

Risks Associated with Vendors and Other Third Parties

16. If the Firm conducts or requires cybersecurity risk assessments of vendors and business partners with access to the Firm's networks, customer data, or other sensitive information, or due to the cybersecurity risk of the outsourced function, please describe who conducts this assessment, when it is required, and how it is conducted. If a questionnaire is used, please provide a copy. If assessments by independent entities are required, please describe any standards established for such assessments.

FIRM - Recommended Actions	RIA WORKSPACE
• Document a vendor management program that includes due diligence before and after contracts are signed. A risk assessment of each vendor should be documented. We recommend focusing efforts on high-risk vendors, defined as companies or individuals who have access to customer data.	• RIA WorkSpace vets out each prior to signing a contract with a new service provider. Vendor risk ratings are reviewed and updated on a regular basis.

17. If the Firm regularly incorporates requirements relating to cybersecurity risk into its contracts with vendors and business partners, please describe these requirements and the circumstances in which they are incorporated. Please provide a sample copy.

FIRM - Recommended Actions	RIA WORKSPACE
• Document a policy or procedures stating that non-disclosure agreements are included in all contracts where vendors may have access to customer or other sensitive information. Formal cybersecurity risk statements should be included in contracts with vendors that process customer transactions.	• See response to #16. • Part of the due diligence process includes evaluation of vendor cybersecurity risk and requirements for non-disclosure agreements.

18. Please provide a copy of policies and procedures and any training materials related to information security procedures and responsibilities for trainings conducted since January 2013 for vendors and business partners authorized to access its network.

FIRM - Recommended Actions	RIA WORKSPACE
• Document any training or security awareness materials provided to vendors.	• Formal training materials are not provided to vendors outside the contract. Vendors that provide professional services to RIA WorkSpace are required to have their own cybersecurity practices that align with RIA WorkSpace requirements.

19. If the Firm assesses the segregation of sensitive network resources from resources accessible to third parties, who (business group/title) performs this assessment, and provide a copy of any relevant policies and procedures?

FIRM - Recommended Actions	RIA WORKSPACE
• Document procedures to manage segregation of all vendor systems used by the firm.	• A formal assessment of network segregation is not performed. However, client networks are completely separated on their own network via their own tenant and their own active directory. By default, all traffic from the outside is denied. • Access control software restricts access to application files residing in the production environment by maintaining separation of duties. • Access to the RIA WorkSpace network is controlled by Microsoft Secure Proxy Servers. Alerts are monitored on a periodic basis. Help desk tickets are created for further investigation.

20. If vendors, business partners, or other third parties may conduct remote maintenance of the Firm's networks and devices, describe any approval process, logging process, or controls to prevent unauthorized access, and provide a copy of any relevant policies and procedures.

FIRM - Recommended Actions	RIA WORKSPACE
• Document a policy regarding remote access to firm systems by vendors. Document procedures for monitoring any such access.	• Access to the RIA WorkSpace network is controlled by Microsoft Secure Proxy Servers based on the business need. Access is granted based on the principle of "least privilege" and “Time Limit”.

Detection of Unauthorized Activity

21. For each of the following practices employed by the Firm to assist in detecting unauthorized activity on its networks and devices, please briefly explain how and by whom (title, department, and job function) the practice is carried out.

FIRM - Recommended Actions	RIA WORKSPACE
• Document procedures for monitoring internally maintained systems and security alerts received from vendors. • Identify personnel within the Firm who are responsible for each activity noted in Question 21.	• Our system architecture ensures network resiliency with redundant power, connectivity, network switching and routing. Data protection includes enterprise-class backup, retention, logging, and secondary site replication. • Logical and physical access is limited based on job responsibility. • Incident response is handled by our Network Operations Center monitoring and responding to these alerts. • Vulnerability scans and penetration tests are performed. • Patches and upgrades are applied regularly based on written policies and standards. • Systems risks are reassessed regularly, and adjustments are made to the control environment, as necessary.

22. Did the Firm update its written supervisory procedures to reflect the Identity Theft Red Flags Rules, which became effective in 2013 (17 CFR § 248-Subpart C-Regulation S-ID)?

FIRM - Recommended Actions	RIA WORKSPACE
• Identity Theft Red Flags Rules are updated when there are changes to the regulations.	• Not Applicable.

23. How does the Firm identify relevant best practices regarding cybersecurity for its business model?

FIRM - Recommended Actions	RIA WORKSPACE
• The firm relies on Microsoft and other software vendors for regular patches and updates to desktop applications. [If the firm has any servers managed completely internally, an additional statement regarding the servers should be included.] • The firm relies on external service providers such as RIA WORKSPACE and {trading broker} for deep technical network and security expertise.	• RIA WorkSpace monitors relevant software vendors (such as Microsoft, Citrix, McAfee, and VMWare) for alerts, patches, and updates. Regular vulnerability scans are performed to help ensure system configurations are kept current.

24. Since January 1, 2013, has your Firm experienced any of the following types of events? If so, please provide a brief summary for each category listed below, identifying the number of such incidents (approximations are acceptable when precise numbers are not readily available) and describing their significance and any effects on the Firm, its customers, and its vendors or affiliates. If the response to any one item includes more than 10 incidents, the respondent may note the number of incidents and describe incidents that resulted in losses of more than $5,000, the unauthorized access to customer information, or the unavailability of a Firm service for more than 10 minutes. The record or description should, at a minimum, include: the extent to which losses were incurred, customer information accessed, and Firm services impacted; the date of the incident; the date the incident was discovered and the remediation for such incident.

FIRM - Recommended Actions	RIA WORKSPACE
• Document a response.	• None noted.

25. Since January 1, 2013, if not otherwise reported above, did the Firm, either directly or as a result of an incident involving a vendor, experience the theft, loss, unauthorized exposure, or unauthorized use of or access to customer information? Please respond affirmatively even if such an incident resulted from an accident or negligence, rather than deliberate wrongdoing. If so, please provide a summary of each incident or a record describing each incident.

FIRM - Recommended Actions	RIA WORKSPACE
• Document a response.	• Not Applicable.

26. For each event identified in response to Questions 24 and 25 above, please indicate whether it was reported to the following:

FIRM - Recommended Actions	RIA WORKSPACE
• Document a response.	• Not Applicable.

27. What does the Firm presently consider to be its three most serious cybersecurity risks, and why?

FIRM - Recommended Actions	RIA WORKSPACE
• Document a response that may include reference to viruses and other malicious software; general hacking; account take-over; identity theft; new vulnerabilities in critical software; keeping up with regulatory requirements; etc.	1. Undocumented vulnerabilities in operating system and network software. These vulnerabilities threaten the overall infrastructure. RIA WorkSpace can only react as new vulnerabilities are announced. 2. Device proliferation and lack of control over end user (mobile) devices. RIA WorkSpace has built a significant control environment for our internal systems but has little to no control over the security configuration of devices used to connect to RIA WorkSpace. End users may not be aware of good security practices. 3. The amount of malware that continues to be developed and propagated through the Internet and lack of end user awareness of the risk of clicking on links in unsolicited messages.

28. Please feel free to provide any other information you believe would be helpful to the Securities and Exchange Commission in evaluating the cybersecurity posture of the Firm or the securities industry.

FIRM - Recommended Actions	RIA WORKSPACE
• Document a response, if appropriate.	• No additional information noted.