Information Security Whitepaper

2021

ISSGOVERNANCE.COM

TABLE OF CONTENTS

Revision History

The author identified is accepted as an electronic signature that concludes this document has been reviewed and approved. The date identified in the "Date Published" column reflects the approval date.

Date Published	Author	Version	Description
09/12/2016	Theresa Hudson	2016Q3 (1.0)	Revised 2.6Most Recent Testing
01/02/2018	Theresa Kitchel	2018Q1 (1.1)	Restructure of documentation Addition of Key Points in several sections Clarification to encryption at rest Appendix A – Updated revision dates Appendix A – Updated revision dates
05/10/2018	Theresa Kitchel	2018Q2 (1.2)	Formatting updates Updated Key Points with current initiatives Added KnowBe4 training Added Data Loss Prevention narrative
06/13/2019	Theresa Kitchel	2019Q2 (1.3)	Formatting updates Added scope section General updates to align with current controls
28 APR 2020	Theresa Kitchel	2020Q2 (1.4)	Updated appendix
29 JUNE 2021	Theresa Kitchel	1.5	Annual review Revised document with current standards Included specifications for additional services Updated layout Removed policy and standard appendices and created separate documents Renamed Cybersecurity Management and Defense System (CDMS) to DLP

1 SCOPE

The purpose of information security policies, and the overall Information Security Management System (ISMS), is to identify controls to safeguard Firm and client information assets and to align the Information security goals and principles with business operations. Specific objectives of this program, and supporting policies and standards, are to:

- Clearly describe management's expectations for employees to protect ISS information assets and those entrusted to us by our clients.
- Define protection requirements for ISS and client information assets.
- Communicate our commitment to providing appropriate levels of protection for information assets.
- Ensure protection is balanced between the value and loss potential of assets with the cost of security measures and mitigating controls.
- Provide the requirements, responsibilities and authorization for implementing and maintaining an effective and efficient ISMS for the Firm.

Controls apply to all office locations, products and services provided by Institutional Shareholder Services and ISS Corporate Services unless otherwise noted. For additional product specific data controls, please contact ISS.

2 INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

Key Points

- Directed globally by the Chief Information Security Officer
- Top down approach with direct communication with ISS Leadership
- Quarterly Information Technology Town Halls
- Weekly Information Security team meetings
- Corporate Security Council (CSC) - Coordinates corporate security initiatives at the executive level to enable the organization to optimize spending, manage infrastructure and minimize security risk.
- Security Task Force (STF) - Coordinates corporate security initiatives and response at the technical level to enable the organization to implement and manage security programs consistent with industry best practices and commitments.

The foundation for developing the Information Security Management System (ISMS) is modeled from the ISO 27001, the international standard addressing information security controls. The ISS ISMS consist of controls for all clauses and control objectives contained in the most recent version of the international standard. This section provides an overview of the Firm's approach to information security and reflects the ongoing commitment to protect information that has been entrusted to the care of ISS.

ISS information security policies are modeled against ISO 27001. Policies apply to all ISS business units, although localized processes and standards may be developed to provide further details on the implementation of these policies. While the Information Security Policies are classified as Internal Use Only and not available for external distribution, an Information Security Binder that contains a list of all our Security Policies and Standards in redacted format (Title, Revision History, Document Information and Contents Pages) is available upon request.

2.1 Management Direction for Information Security

The goal is to ensure adequate protection of client and ISS information assets in accordance with internal policy controls, business requirements, and relevant laws and regulations. The information and controls contained in the ISMS support the commitment to and are intended to exemplify clear management direction for information security at ISS.

2.2 Responsibilities

The Information Security Office (ISO), with cross-functional support, is responsible for establishing and maintaining information security policies and standards for the Firm. Business units are responsible for ensuring the implementation of controls within their respective areas of responsibility. Each user is responsible for abiding with the intent of controls to protect Firm assets and those of the clients.

2.3 Risk Management

Key Points

- Risk Management Program – Risk Review Board (RRB) hold a monthly review of identified risks, ensuring remediation and mitigation processes stay on target.
- Change Management Program – The Change Approval Board (CAB) hold weekly meetings to review and approve all emergency or planned changes to the production environment. The CAB along with the change owner are jointly evaluating all changes for risk and consequence.
- Vulnerability Management Program - Key Information Security and Information Technology members attend a monthly vulnerability meeting to ensure scans are reviewed, vulnerabilities are assessed for risk to ISS and the patch cycle/content is adjusted as needed.
- Threat Intelligence Information Security collects information from a range of sources such as Intel Security/McAfee, NIST, SEC, SANS, and Homeland Security for intelligence gathering purposes. This includes cyber threat intelligence, geopolitical cyber threats, government, industry, commercial and internal/external intelligence sources. The information is used to assess the environment and determine any new or continuing risk to the company.

In addition to the formal risk management program, ISS incorporates risk reviews in other key areas to ensure risk has a holistic view. The Information Security Office reviews and manages technical and operational risks to the services provided to clients and reviews any mitigation efforts and reports those activities to ISS management teams.

Risk assessments are performed regularly to address changes in the information security requirements and when significant changes occur. ISS performs risk assessments on a variety of assets within the organization. These include physical assets, people, processes, software, and information.

2.4 Organization of Information Security

The Information Security Office is directed globally by the Chief Information Security Officer and is supported by local IT and business stakeholders around the Firm. ISO is responsible for information security, physical security, business continuity, disaster recovery and cybersecurity. These core focus areas are leveraged to maintain the ISS control framework. The ISMS is supported by technical expertise of IT infrastructure teams who work closely with the Information Security Office. ISS also engages third-party expertise to ensure a current view of worldwide security issues and industry best practices is maintained.

2.5 Personnel Security

Key Points

- Central change request system ensures new hire, termination and change in job role requests are handled consistently.
- Security awareness training including formal security policy acknowledgement provided for new hires with an annual refresher course.
- Role-based training and continuous phishing test campaigns provide on-going awareness and reinforcement.
- Monthly security awareness announcements
- ISS' Code of Conduct ensures employees are aware of data privacy requirements including restrictions on sharing non-public information with anyone outside the company. Employees are also prohibited from sharing such information with anyone inside the company unless with another employee who needs such information to perform their duties.
- Monitoring controls allows ISS to more efficiently assess the control environment.

The ISS Human Resources department ensures background checks are performed for all new hires, prior to the first day of employment. Background checks generally include criminal history, Social Security number traces, educational verification and past employment verification. All new employees are provided a new employee package that details ISS' core corporate and security policies.

ISS maintains a security awareness program that includes mandatory training, policy acknowledgement and assessments. New employees are required to complete security awareness training upon being hired, and annually thereafter.

Managers are responsible for ensuring users within their areas of responsibility apply appropriate information security controls. ISS policies contain statements regarding disciplinary actions, up to and including termination of employment for committing a security breach, or not complying with information security controls

Policy controls have been developed to address processes associated with terminating users' employment and users changing job roles or function. Processes for access revocation or modification are in place and employees separating from the Firm are required to return all information assets belonging to ISS upon termination.

2.6 Information Asset Management

Key Points

- Global Asset Register
- LanSweeper – asset reconciliation
- SCCM – configuration management
- Wisdom – application register
- CAT Tools – network device tracking
- Tenable – asset reconciliation
- Regular review of assets
- Information Classification
- Secure destruction of assets

ISS maintains a global asset management program that is used to track hardware and software. Endpoint security tools and Systems Center Configuration Manager (SCCM) software are used to assist with and automate information asset management controls.

A policy defining acceptable use of information assets is in place. Users are reminded of acceptable use guidelines and requirements during annual Ethics training and Security Awareness training.

Information is classified into four categories: *Public, Internal Use Only, Confidential* and *Restricted.* Each classification is based on the value and risk factors of the information being classified. Non-public client data is classified as *Confidential*.

Information asset handling requirements have been identified for each classification and include guidance for: storage, transmissions, distribution, physical security, destruction, disposal, recycling, reuse, duplication, and security logging, monitoring and auditing

ISS has implemented both administrative and technical controls to govern and manage removable media. Administrative controls include policy and standard requirements while technical controls are in place to ensure users are unable to copy data onto removable media such as a CD or DVD. USB devices are wholly encrypted and only available for use on another ISS-protected machine. Once encrypted, USB devices are unreadable from any non-ISS device and are scanned by endpoint protection when connected.

Processes have been implemented to ensure media that has reached "end-of-life" is securely wiped using DOD standards prior to the media being destroyed. When destruction is performed by a third party, ISS maintains chain of custody and certificate of destruction records.

2.7 Access Controls

Key Points

- ISS monitors access to information by maintaining and reviewing audit trails. ISS' Information Security Office utilizes role-based access controls to identify, authenticate, and authorize individuals to access systems based on their role. This group also applies the use of technology such as firewalls and IP based permissions, to limit connectivity to ISS' hosted services and applications along with protection and encryption of confidential data for secure communication.
- Access to client data is restricted to authorized employees based on their job role. Authorization is granted on a need-to-know and least privilege basis. In addition, ISS has policies and procedures regarding confidentially contained in its Code of Conduct.

The Access Control Policy identifies requirements for controlling access to ISS and client information assets. Access is authorized based on the principles of least-privilege and need-to-know, and role-based access controls identify and authorize users based on their respective roles. Privileged user accounts are not used for day-to-day access of core applications.

Access is provisioned (and de-provisioned) following documented processes that ensure that access is requested, approved, and implemented as appropriate for users. Unique user IDs and password combinations are used to provide authentication and individual accountability. Authentication is based on a minimum of strong, complex password comprised on alphabetic, numeric and special characters.

Passwords are configured to expire at regular intervals. Additional technical controls have been implemented to ensure accounts are locked after 5 consecutive failed logon attempts and workstations and systems auto-lock after a 10-minute period of inactivity.

User access rights are reviewed at regular intervals during access control audits. These activities are used to ensure the effectiveness of the processes in place for disabling access upon termination or other separation from the Firm.

2.8 Cryptography

Key Points

- Storage at rest meets FIPS 140-2 Level 1
- Backup encryption meets AES 256-bit (CBC) FIPS 140-2 Level 1
- Email encryption communication supports opportunistic TLS for the protection of email traffic with TLS1.2 as the preferred method of connection.
- Endpoint AES 256-bit (CBC) encryption on systems which can be accessed outside of an ISS facility.
- Application access restricted to https providing transmission encryption.
- SFTP communication available for delivery of information.

Cryptography at ISS is centrally managed by the IT Infrastructure organization. A cryptography policy has been implemented to govern the use of cryptographic controls needed for the protection on information. This includes ensuring web interfaces are appropriately protected with SSL certificates and ensuring appropriate encryption is implemented for data at rest.

2.9 Physical and Environmental Security

Key Points

- Datacenters are in natural disaster “safe zones”.
- CCTV video monitoring in place for office and datacenter locations.
- Physical security badging system provides access established using the principles of least-privilege and need-to-know.
- Access to datacenters is restricted to a specified list of individuals who have been pre-approved. All datacenter visits require advance notice.
- UPS and generator power for continuity at office and datacenter locations.
- Environmental controls to ensure the safety of personnel including fire detection systems.
- Regular reviews and updates of building security including drills for applicable environmental situations such as tornado, hurricane, and fire drills.
- Business Continuity planning captures pandemic planning in case of any mass illness.

ISS hosts its web applications and services from datacenters in the United States and the United Kingdom (UK) based on client operations and legal and contractual agreements. ISS’ datacenter facilities and physical security systems were designed to provide extremely hardened, state-of-the-art, secure operational locations.

US DATACENTERS

SWITCH

ISS contracts with Switch for rack spaces, power, environmental and network services for the hosted applications and services. ISS does not share company data, client data or access to such data with Switch. The infrastructure is hosted in highly secure, Tier IV datacenter facilities.

Considerable physical security controls are in place, with well-defined perimeters, blast walls and gates, clear avenues of approach and secondary perimeter barriers. Exterior doors of the datacenter lead to specially engineered mantraps built over a fire corridor wall construction. All access points of the mantraps require additional biometric authentication of the access card holder and are controlled by 24x7 Security Officers and man-trap relay logic.

ISS physical access controls provide additional protection by the positive access control procedures deployed at the facilities. Positive access control requires that officers in the Security Command Center, staffed 24x7, verify each person gaining access matches a file photo. After confirmation, the officer activates the second proximity and biometric readers.

Equipment being transferred in and out of the facility is logged by facility management personnel to track environment and power needs. Additionally, equipment is transferred through a special receiving mantrap to manage secure delivery to, or extraction from, the protected environment.

Switch provides start-of-the-art environmental systems in the datacenters. Fire protection includes fire, smoke and heat detection solutions that are monitored 24 hours a day. Sensors are located throughout the datacenters and provide alerts to both infrastructure and physical security personnel for appropriate response. Datacenters are also protected with aspirating smoke detectors that are capable and programmed to identify smoke at the incipit stage. Additionally, datacenters are equipped with dry-pipe sprinklers.

Datacenters utilize multiple inbound connections from utility providers. A triple-redundant power source, which balances dual inbound power connection across three sources of power, optimizes power utilization. Backup power is provided by more than 20 uninterruptible power supply (UPS) devices and 19 diesel-powered generators across the campuses. Power distribution units are managed and secured to prevent tampering. AC and DC cables within the datacenters are color-coded for quick and succinct identification of circuit and power feeds.

AMAZON WEB SERVICES (AWS)

Details on AWS datacenter security controls can be found at:

https://aws.amazon.com/compliance/data-center/controls/

UK Datacenters

SUNGARD

ISS contracts with SunGard Availability Services in the United Kingdom for both primary and disaster recovery datacenters.

Network access is redundant with delivery along diverse paths for high-availability routing of communications. Triangulated connectivity to multiple SunGard Availability Services; datacenters provide greater diversity and resilience of communications providers. ISS connects to the UK datacenter via the established MPLS network, with internet service provider (ISP) backup connections.

Physical security controls are in place, with well-defined perimeters, blast walls and gates, and clear avenues of approach. External and Internal CCTV cameras provide monitoring and digital recording that is saved to disk. A proximity-based access control system is in place to govern ingress to the facilities. Security guards are on-site 24x7 and physical security is supplemented by intruder and door alarms with external infrared detection.

There are two main power feeds for each datacenter and the facilities are configured with a minimum of “N+1” power redundancy. There are diverse A and B power supplies in each ISS-dedicated cabinet. Additionally, ISS equipment is protected with over 20 UPS units and on-site backup diesel generators that will sustain required power in the event of a power outage. 72 hours of fuel is stored on site for the generators with emergency provisions in place for extra fuel, if needed.

Fire suppression in the datacenter is achieved through pre-action, dry pipe systems and early warning VESDA (air sampling) smoke detection and alarm systems. VESDA systems are approximately 100 times more sensitive than conventional fire detection systems. Temperature and humidity controls and sensors are also employed to monitor the environment.

OFFICES

ISS maintains controls for office security and personnel safety. Physical security controls ensure offices are safe which include restricted badge access and visitor procedures and all staff working areas are separate from public meeting rooms. Building management provides security personnel for exterior and general building security. CCTV monitoring in most office locations cover egress, ingress and sensitive areas, with data retained for at least a minimum of 30 days. Environmental controls ensure the safety of personnel including fire detection systems and include drills for situations such as tornado, hurricane, and fire drills where applicable.

Business Continuity planning captures pandemic planning in case of any mass illness.

Users must lock or logoff workstations, systems or applications before leaving unattended. All ISS computer equipment has a screen saver enabled after 10 minutes of inactivity and requires a password to unlock the computer.

Clear desk and screen policy indicating users may not leave documents, printouts, removable media or other information assets containing sensitive data unattended. Sensitive information assets not in use must be stored in a locked office, drawer or file cabinet.

2.10 Operations Security

Key Points

Malware protection at multiple points:

- Endpoint protection covers anti-spam, phishing and malware which is applied throughout the organization and updated multiple times a day.
- Email gateway detection files are updated daily from vendors ensuring up-to-date protection against phishing attempts, spam, and malware.
- Web gateway provides content filtering to prevent access to prohibited websites or those that are highly suspected of current or past virus activity and safeguard the internal network from Internet-borne threats such as spyware, viruses and other malware.
- Backup programs provide encrypted backups in both the production datacenter for rapid recovery as well as the disaster recovery datacenter for continuity purposes.
- Production servers, networks and applications are monitored 24x7x365 by fully automated monitoring and alerting systems.
- A central NTP server is used to accommodate time synchronization across all networked devices.
- Vulnerability Management Program ensures patching guidelines are established, weekly network vulnerability and regular application scans are performed, and annual penetration testing is conducted.

Operational standards for the secure operation of information processing systems are implemented and maintained. These standards include appropriate operating procedures, change management controls, and documented requirements for the segregation of duties and environments.

ISS protects Firm and client information assets by maintaining and managing prevention, detection and recovery controls for malicious software (malware). Approved anti-malware software that provides on-access scanning capabilities has been deployed and is installed on ISS endpoints. Additional malware protection is in place through the email gateway and web gateway deployments.

A dual backup approach is employed at ISS datacenters. At the primary production datacenter, data is backed up locally as well as being replicated to the DR (failover) datacenter. Full backups are performed monthly, and incremental backups are performed nightly. Monthly full backups are maintained on storage that has the capacity to store the backup data as required per regulatory and contractual obligations.

IT personnel monitor the success or failure of backups and are notified of backup job statuses via email. Backup restoration tests are performed regularly to verify that production data can be recovered from backup files. Backups are appropriately protected during the replication activities and at rest.

ISS has systems in place which collect and analyze logs from applications, operating systems and network devices. Application logs are collected via centralized log management platforms. Operating systems and network device layers are also centralized, with priority targets ultimately being forwarded to the Security Information and Event Manager (SIEM). The secure log management applications consolidate and automate event log archiving and incident alerting across critical production systems.

Production servers, applications and networks are monitored 24x7x365 by fully automated monitoring and alerting systems. Monitoring includes up/down status, disk utilization, network utilization and processor utilization for servers and the key services they perform. Historical performance monitoring is also maintained for analysis of system performance over time.

Vulnerability scans and patch management are critical components of the ISS vulnerability management program. Scans of ISS' perimeter Internet facing networks and internal infrastructure are performed weekly. Results of these scans are distributed to appropriate stakeholders for remediation. Penetration testing by an independent third party is performed annually on chosen web applications and externally facing infrastructure.

IT and the Information Security Office are notified of new security vulnerabilities by industry alerts, automatic notification received through vendors, subscription services or other verifiable sources such as SANS or the CERT Coordination Center.

The ISS patch cycle is determined on two criteria: criticality and operating system and application cadence. All patches and updates to network devices adhere to the standard ISS change control process. If the patch or update is intended to address a security issue, it is tested and then deployed to the production environment at the earliest timeframe allowed by the change control process. The general guidelines are endpoints and production environments are updated monthly and the lower environments are updated daily.

Key Information Security and Information Technology members attend regular vulnerability meetings to ensure scans are reviewed, vulnerabilities are assessed for risk to ISS and the patch cycle/content is adjusted as needed.

2.11 Communications Security

Key Points

- Networks are designed with multi-zoned security architecture controlled by firewalls between tiers.
- Email DLP controls proactively detect the presence of sensitive information.
- McAfee DLP provides host-based protection
- Remote access to the ISS network is requires approved remote access software and Okta Verify to enforce multi-factor authentication of users.
- Access to production datacenter assets is restricted to approved privileged accounts and requires multi-factor authentication.
- Mobile Device Management software is used to secure mobile devices.
- Removable media protection disables CD/DVD write capabilities and encrypts USB drives for only ISS endpoint access.

A global MPLS network connects all ISS offices in a secure, private network. Additional network security controls include:

- A multi-zone security architecture that ensures all data flows are controlled by firewalls between application tiers and between different applications:
  - Tier 1 – Load Balanced Web Servers
  - Tier 2 – Application and Analytic Servers
  - Tier 3 – Database Servers
- Firewall rules which are reviewed and approved prior to implementation.
- Firewalls which only allow the network traffic necessary for the applications to operate and be managed.
- Restricted access to administrative network devices by authorized IT personnel only.
- Continuously monitoring endpoints.

ISS maintains a global asset management program that is used to track hardware and software. Endpoint security tools and Systems Center Configuration Manager (SCCM) software are used to assist with and automate information asset management controls.

SECURE CONNECTIVITY

EMAIL SECURITY

The email environment supports opportunistic Transport Layer Security (TLS) for email delivery for remote email servers which advertise MTA capability.

SECURE INTERNET ACCESS

ISS protects the internal network from Internet-borne threats such as spyware, viruses and other malware by use of advanced web filtering technology that operates at the point of egress for all Firm network traffic to the Internet. In addition to stripping all standard viruses and spyware, URL access is filtered to block content deemed to be inappropriate.

REMOTE CONNECTIVITY

ISS provides remote access for employees that may require this type of access to support their job role or for business continuity purposes. Controls are implemented at ingress and egress points to the global Wide Area Network (WAN) and multi-factor authentication is required. Additional controls and guidance for staff working remotely include but are not limited to:

- Training and education on secure remote working practices and company policies before remote access is provided.
- Full disk encryption on company laptops.
- Approved remote access via Cisco AnyConnect VPN or VMWare Horizon.
- Mobile Device Management (MDM) software is used to provision and secure ‘Bring Your Own Device’ mobile devices.

2.12 System Acquisition, Development and Maintenance

Key Points

- Formal change control process
- Separation of duties

Formal change control procedures are maintained to protect the integrity of information assets, systems and applications in the production environment. Testing of applications is performed in a controlled testing environment. Test data is carefully selected and controlled.

A standard change control process is followed when implementing changes to systems and applications. The following items are addressed by change controls procedures:

- Impact analysis (including dependent systems and applications and users)
- Testing requirements (test plans, results, acceptance, roll-back procedures)
- Approval and acceptance of procedures
- Notification procedures
- Documentation requirements
- Separation of duties among the different environments (Development, UAT, QA, Production)

Required approval level for emergency changes to the production environment.

2.13 Vendor Relationship Management Program

Key Points

- Approved vendor list
- Risk assessment and vendor tiering
- External validation of vendor cybersecurity controls

A vendor relationship management program is in place to minimize risk that may be experienced by engaging an external provider. Vendors are tiered using various risk-related criteria. Depending on the risk score, various methods are used to evaluate external providers, including a combination of the vendor’s security program and controls, reviews of independent validation of controls, contractual requirements, and responses to the ISS information security assessment questionnaire. At all times, the goal is to ensure the continued protection of information assets belonging to the Firm and information entrusted to us by our clients.

2.14 Incident Management

Key Points

- Central tracking
- Corporate Security Council review
- Regular review meetings

ISS maintains an Information Security Incident Response Policy and plan that requires incidents to be reported, acted upon, escalated, and resolved in a timely manner. To ensure cross-functional teams across the Firm can support this policy, an Incident Response Plan has been implemented to provide repeatable and reliable steps for responding to information security events and incidents that may occur.

The Incident Response Plan provides comprehensive instructions for handling all phases of event and incident response. These phases include *Identification*, *Notification*, *Triage*, *Verification*, *Containment*, *Eradication*, *Recovery* and *Post-Mortem*. Specific roles and associated responsibilities are defined. The Incident Response Plan also includes processes for client notifications that may be required if an incident results in a breach of client information. Clients will be notified if their information is directly involved in a breach.

2.15 Independent Reviews

ISS undergoes several audits on an annual basis that are performed by an independent third parties. These reports are available to clients upon request through the Client Services team.

SSAE18 SOC1 TYPE II

Scope: ProxyExchange (PX), GPD, RecoverMax (SCAS), and the supporting infrastructure and operations.

This is a detailed and comprehensive audit consisting of 50 activities in five key control areas:

- Access Control
- Backup Operations
- Configuration and Change Management
- Operations and Communications Security
- Physical and Environmental Security

SSAE18 SOC2 TYPE II

Scope: Beacon, Local Market Share (LMS),

This is a detailed and comprehensive audit consisting of 50 activities in five key control areas:

- Access Control
- Backup Operations
- Configuration and Change Management
- Operations and Communications Security
- Physical and Environmental Security

ISO 27001

Scope: Financial Clarity and Mortgage Clarity

This is a detailed and comprehensive audit consisting of 114 controls in fourteen key control areas

2.16 Compliance

All employees and non-employees are expected to comply with ISS policies and controls. Provisions and processes for non-compliance are in place and, depending on the severity, may result in disciplinary action, up to and including termination of employee, contract or agreement.

3 DATA LOSS PREVENTION (DLP)

Key Points

Complete Data Protection Suite (ePO)

- Endpoint security (anti-malware and anti-spam)
- Endpoint encryption
- Removable media control

Email Gateway

- Anti-malware and anti-spam protection
- Whitelist/Blacklist functionality
- Mimecast, O365 Security and Compliance Center and McAfee DLP provide threat management depth
- Compliance email and instant message archival

Web Gateway

- Network web protection
- Permitted categories

Enterprise Security Manager (SIEM)

- Real-time visibility into activity on systems, networks, databases and applications.
- Alerts and Reports

Vulnerability Management

- Scheduled scans encompass all office locations and datacenters
- Ad-hoc basis performed when necessary
- Database Security Scan improves visibility into, and limits exposure of, database data.

ISS has leverages existing controls and tools that work in concert to support the Data Loss Prevention (DLP) program.

ISS continually invests in security tools and technologies in support of its information security and cybersecurity programs.

DLP is done at two levels – gateways and host based. The controls in place at email, web and network level work together to detect and prevent confidential data from being distributed out of the organizational boundaries for unauthorized use.

3.1 Security Tools

COMPLETE DATA PROTECTION SUITE

This suite of tools provides advanced data protection from risk of loss, theft, and exposure using a combination of powerful enterprise-grade endpoint encryption, access control, and user-behavioral monitoring. These tools assist ISS in establishing and enforcing information protection and centralizing information security management using a single management console. The suite integrates strong encryption, authentication, access control, data loss prevention, and policy-driven controls.

COMPLETE ENDPOINT PROTECTION SUITE

The Complete Endpoint Protection Suite provides strong, fast and scalable defense for ISS devices. The suite provides advanced endpoint protection for ISS that includes hardware-enhanced security against stealthy attacks, behavioral anti-malware and dynamic whitelisting in addition to the essential anti-malware, anti-spam, web security, and firewall and intrusion prevention. These comprehensive tools extend threat protection to data and the systems with the ability to find, fix and freeze malware fast. The security approach covers all bases, layering hardware-enhanced technologies, dynamic whitelisting, smart scanning, advanced anti-malware, mobile protection and more.

CONTENT SECURITY SUITE

This set of tools combines Web Protection, Email Protection, Network Data Loss Prevention, and Device Control into a unified suite. This approach provides ISS the right security to protect ISS and client data from today's inbound and outbound threats such as:

- Protection against blended and targeted malware attacks.
- Integrated email protection to eliminate spam, malware, phishing attacks and other email-borne threats.
- Web security provides protection to allow ISS users to navigate the web safely without fear of phishing, spyware, targeted attacks and data loss.
- Achieve industry and regulatory compliance about risk management and technical compliance.

SERVER SECURITY SUITE

The Server Security Suite provides foundational server security protection and management for physical and virtual deployments, enabling ISS to discover workloads for complete security visibility, protect workloads with desired security policies, and expand workloads with automatic provisioning of security policies.

ENTERPRISE SECURITY MANAGER (SIEM)

Effective security starts with real-time visibility into all activity on all systems, networks, databases and applications. The Enterprise Security Manager provides true, real-time situational awareness and the speed and scale required to identify critical threats, respond intelligently, and ensure continuous compliance monitoring.

Global Threat Intelligence provides valuable, real-time information on external threats gathered from hundreds of millions of sensors around the world, allowing ISS to pinpoint malicious activity on the network. The Enterprise Security Manager can leverage Global Threat Intelligence to quickly identify any time an internal host has communicated with a known "bad actor", or malicious external device.

TENABLE SECURITY CENTER AND .IO

The Vulnerability Manager, with its Asset Manager feature, delivers unrivaled scalability and performance by actively or passively canvassing every device connected to the ISS network. ISS can uncover devices hidden on the network as well as smartphones, tablets, and laptops that come and go between scheduled scans. If it has an IP address or is using the network, the Vulnerability Manager can discover and assess it, automatically or on a schedule, revealing the compliance of all assets on the network.

NEXT-GENERATION FIREWALLS

Next-Generation Firewalls integrate security features with high availability and manageability, delivering advanced network protection across the entire enterprise. These Next-Generation Firewalls integrate application control, intrusion prevention system (IPS), and evasion prevention into a single solution.

High availability and scalability support the security demands of datacenters that need to deliver uninterrupted uptime with no gap in protection.

CISCO FIREPOWER IPS

High availability and scalability support the security demands of datacenters that need to deliver uninterrupted uptime with no gap in protection.

4 BUSINESS CONTINTUITY MANAGEMENT SYSTEM (BCMS)

Key Points

- As of December 31, 2020, ISS has 29 global locations in 15 countries which provides ISS with the ability to transfer work processes from one location to another seamlessly in most cases. This strategy is a common scenario for both short and long-term planning dependent on time of year and impacted office locations.
- ISS maintains disaster recovery datacenters which could be initialized if a DR event was declared.
- ISS maintains a work remote/work from home strategy for personnel for business continuity events. Crisis management teams are defined for each office location, typically including at minimum the Head of Office, Office Manager, Local IT, and Information Security personnel.

ISS is committed to providing clients with timely and dependable access to the products and services and have taken aggressive steps to prepare for contingency situations under a variety of potential scenarios. ISS continues to evolve the Business Continuity Management System (BCMS) and expand the resources to provide timely recovery of critical business operations in the event an unplanned interruption occurs. The BCMS is supported by cross-functional teams representing each of the global offices. Plans within the BCMS are reviewed and tested on an annual basis. Plans are updated as needed to compensate for changes to products, services, business processes and infrastructure.

4.1 Business Impact Analysis

An annual Business Impact Analysis (BIA) determines levels of criticality, risks, and operational requirements needed to provide critical products and services. A BIA has been completed for each critical operational function and support capability in each of the global offices. The results of the BIA exercises have identified critical business operations that may need to be transferred from one global office to an alternate global office in the event of an extended, localized outage.

4.2 Business Continuity Plans

ISS maintains Business Continuity Plans (BCPs) that identify response team members, roles and responsibility, operational considerations and contact directories with cascading call trees. The BCPs include the following elements:

- Plan Overview
- Plan Requirements
- Roles and Responsibilities
- Local Office and IT Information
- Business Impact Analysis
- Recovery Objectives
- Business Continuity Plan
- Runbooks

4.3 Disaster Recovery Plans

For extended information technology-related outages, the Disaster Recovery Plan may be invoked. Meeting the business Recovery Time Objective (RTO) and Recovery Point Objective (RPO) is the focus of this Plan. Technical response will depend on the scope and scale of the incident. In the event of a catastrophic loss of a primary datacenter, systems, applications and storage will be failed over to the alternate DR datacenter. ISS has technical teams in North America, Europe and Asia. These teams will recover production systems and applications in the event a team in a geographical area is unavailable.

Critical production services include redundant and highly available network components within their architecture, with backup power, UPS and on-site power generators. All production data is backed up locally within the production datacenter using electronic storage, and all production data is asynchronously replicated to the alternate DR datacenter.

RECOVERY OBJECTIVES

In the event of a complete datacenter failure, the Disaster Recovery Plan will be invoked, and ISS will initiate failover to the alternate DR datacenter. Production applications will be restored in order of priority with full normal operations expected within the recovery time designated for the services provided.

4.4 Crisis Management Plan

As part of the BCMS, ISS has a formal Crisis Management Plan. The Plan includes Crisis Management Teams that are comprised of cross-functional groups drawn from each of the offices and leadership team from each of the lines of business. Appropriate plans and teams are ready to be engaged for any situation that has an impact on the staff, buildings or infrastructure of ISS, or any situation that has a significant impact on daily operational capabilities.

Ongoing coordination and communication is described throughout the plan via teleconference bridges, websites, email and phone messaging systems. Communications to the clients will be managed by the Information Security Office and dedicated Client Service teams. Clients will be continually updated throughout the crisis via the account management and client service points of contact.

COMMUNICATIONS

As with all major events, communication is key. To support continued communications, ISS follows these high-level objectives:

- Immediately update ISS employees on the current situation.
- Continue to provide updates to employees as the situation evolves, leveraging email and web-based updates.
- Distribute region-specific advisories, as appropriate.
- Formulate communication to clients regarding the ISS response to the event.
- Verify systems are ready for a mass-client email, if deemed to be necessary.
- Provide additional communications to clients and shareholders if the situation escalates.

4.5 Pandemic Plan

There are a variety of scenarios that might lead to staff unavailability, including a widespread outbreak of an illness or infectious disease. ISS has a plan designed to support the goal of protecting the employees during a pandemic event. The three objectives for the pandemic planning are employee well-being and support, service continuity, and communications.

EMPLOYEE WELL-BEING AND SUPPORT

The well-being of the employees is of critical importance. Upon warning or notification of a pandemic event, the following activities may be considered:

- Reinforcement and addition of existing healthy habits already published.
- Communication of policy on self-isolation if an employee or family member does not feel well.
- Review HR policies on working from home, parental time off, sick and vacation days to prevent sick employees from feeling forced to come to the office.
- Publish additional advisories based on “high level” regional developments.
- Review Travel Policies considering recommendations from authorities such as the CDC, WHO and the State Department. No forced travel.
- Review information related to vaccinations and provide employees information and advice as needed.

SERVICE CONTINUITY

ISS is committed to maintaining the capability to provide products and services to the clients during a Pandemic event. The following high-level objectives have been identified for Pandemic service continuity:

- Leverage existing BCMS framework.
- Engage response teams to review status and potential scenarios which may include:
  - A potential drop in productivity
  - Prolonged periods of employees working from home
  - Impacts of widespread disruption to transportation services
- Review key deliverables.
- Business leaders are responsible for reviewing scenarios and advising on potential business impacts.

4.6 Information Security aspects of Business Continuity Management

Information security controls, tools and technologies have been included in ISS Business Continuity and Disaster Recovery plans to ensure appropriate controls are maintained in the event of an adverse situation. Similarly, high availability and failover capabilities have been implemented from an infrastructure perspective. These activities work in concert to ensure ISS can sustain operational and support capabilities in the event of an unplanned, extended outage.

4.7 Testing

ISS finds testing various components of the program on a continuous basis allows teams to ensure preparedness across the firm and allow for quick action to any adjustments in processes that may be needed. Using this logic, ISS tests components of the program every month. Example of tests include:

- Testing the ability to failover and failback databases which support applications.
- Testing remote continuity planning, VPN availability and stability for various office locations.
- Failover to the disaster recovery datacenter and failback to the primary datacenter.

Lessons learned are tracked through the testing report as well as the central change management system, JIRA.

ISS

We empower investors and companies to build for long-term and sustainable growth by providing high-quality data, analytics, and insight.

GET STARTED WITH ISS SOLUTIONS

Email sales@issgovernance.com or visit issgovernance.com for more information.

Founded in 1985, the Institutional Shareholder Services group of companies ("ISS") is the world's leading provider of corporate governance and responsible investment solutions alongside fund intelligence and services, events, and editorial content for institutional investors, globally. ISS' solutions include objective governance research and recommendations; responsible investment data, analytics, and research; end-to-end proxy voting and distribution solutions; turnkey securities class-action claims management (provided by Securities Class Action Services, LLC); reliable global governance data and modeling tools; asset management intelligence, portfolio execution and monitoring, fund services, and media. Clients rely on ISS' expertise to help them make informed investment decisions.

All statistics referenced in this document are updated on an annual basis and, unless otherwise noted, relate to the year ending December 31, 2018.

This document and all of the information contained in it, including without limitation all text, data, graphs, and charts (collectively, the "Information") is the property of Institutional Shareholder Services Inc. (ISS), its subsidiaries, or, in some cases third party suppliers.

The Information has not been submitted to, nor received approval from, the United States Securities and Exchange Commission or any other regulatory body. None of the Information constitutes an offer to sell (or a solicitation of an offer to buy), or a promotion or recommendation of, any security, financial product or other investment vehicle or any trading strategy, and ISS does not endorse, approve, or otherwise express any opinion regarding any issuer, securities, financial products or instruments or trading strategies.

The user of the Information assumes the entire risk of any use it may make or permit to be made of the Information.

ISS MAKES NO EXPRESS OR IMPLIED WARRANTIES OR REPRESENTATIONS WITH RESPECT TO THE INFORMATION AND EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES (INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF ORIGINALITY, ACCURACY, TIMELINESS, NON-INFRINGEMENT, COMPLETENESS, MERCHANTABILITY, AND FITNESS for A PARTICULAR PURPOSE) WITH RESPECT TO ANY OF THE INFORMATION.

Without limiting any of the foregoing and to the maximum extent permitted by law, in no event shall ISS have any liability regarding any of the Information for any direct, indirect, special, punitive, consequential (including lost profits), or any other damages even if notified of the possibility of such damages. The foregoing shall not exclude or limit any liability that may not by applicable law be excluded or limited.

ISSGOVERNANCE.COM