Information Security Whitepaper

Institutional Shareholder Services

June 2019

PRESENTED BY

Institutional Shareholder Services Inc.
702 King Farm Boulevard, Suite 400
Rockville, Maryland 20850

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	Revised 2.6 Most Recent Testing
01/02/2018	Theresa Kitchel	2018Q1	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	Formatting updates Updated Key Points with current initiatives Added KnowBe4 training Added Data Loss Prevention narrative
06/13/2019	Theresa Kitchel	2019Q2	Formatting updates Added scope section General updates to align with current controls

TABLE OF CONTENTS

1. SCOPE

The purpose of information security policies, and the overall Information Security Management System (ISMS), is to identify controls that help to safeguard Firm and client information assets and to align the goals and principles of information security with ISS 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 services provided by Institutional Shareholder Services and ISS Corporate Services.

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
- Security presentations at office staff meetings
- Quarterly Information Technology Town Halls
- Weekly Information Security team meetings
- Quarterly 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.
- Quarterly 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 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, Appendix A of this whitepaper contains the tables of content and document history/approval for each policy document.

This suite of policies is supported by issue-specific information security standards for which the tables of content and document history/approval is included in Appendix B of this whitepaper.

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. 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.

3. Risk Management

Key Points

ISS incorporates assessing risk in many of the key areas owned by Information Security and Information Technology. Keys areas include (not all inclusive):

- Change Approval Board (CAB) – Weekly meeting to review and approve all emergency or planned changes to the production environment. The CAB along with the change facilitor are jointly evaluating all changes for risk and consequence.
- Vulnerability Management Program - Key Information Security and Information Technology members attend a weekly vulnerability meeting to ensure scans are reviewed, vulnerabilities are accessed for risk to ISS and the patch cycle/content is adjusted as needed.
- Self-Assessment – Information Security utilizes many organizations for information gathering such as Intel Security/McAfee, NIST, SEC, SANS, and Homeland Security. The information is used to assess the environment and determine any new or continuing risk to the company.

The Information Security Office (ISO) reviews and manages technical and operational risks to the services provided to clients. ISO reviews and manages operational risk to the firm, reviews any mitigation efforts and reports those activities to ISS management teams.

Risk assessments are performed periodically 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 may be physical assets, people, processes, software, and information.

4. Organization of Information Security

The Information Security Office is directed globally by the Chief Information Security Officer and is supported by several 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.

5. Personnel Security

Key Points

- Central change request system ensures new hire, termination and change in job role requests are handled consistently.
- KnowBe4 Security Awareness Training (K-SAT) – Provides security awareness training for new hires, annual refresher course, role-based training and phish testing.
- KnowBe4 Phishing training providing continuous reinforcement of training.
- KnowBe4 Compliance Manager (KCM) – Provides a control management solution allowing ISS to more efficiently assess the control environment.
- Security presentations at office staff meetings
- Periodic all staff emails refreshing key elements of the security awareness training.

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 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 on or prior to their last day of employment.

6. Information Asset Management

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 home PCs or any non-ISS device.

Processes have been implemented to help 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.

7. Access Controls

Key Points

- ISS' Regulatory Code of Ethics specifically addresses this issue and provides that employees who are privy to non-public proxy voting recommendations are prohibited from sharing such 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.
- 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 stateful inspection 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.

- The roles which have authorization to access client data include database administrators who have responsibility for administering client databases and client service personnel who have responsibility to service the client account. In addition, ISS has policies and procedures regarding confidentially contained in its Regulatory Code of Ethics.

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 every 60 days. 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 least semi-annually 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.

8. Cryptography

Key Points

Key areas of data encryption include:

- Storage at rest: Meets FIPS 140-2 Level 1 requirements within the US datacenters.
- Backup: Meets AES 256-bit (CBC) FIPS 140-2 within the US datacenters.
- Email: Opportunistic email encryption via TLS for the protection of email traffic. Currently TLS 1.2 is preferred, TLS 1.0/1.1 are enabled but de-prioritized.
- Device: All ISS devices that operate outside of secure ISS facilities are AES 256-bit (CBC) encrypted.
- Application access: Applications are available only via https to ensure that all application data is encrypted before transmission.
- Client communication: Clients have the option of using ISS ftp or sftp server for delivery of reports depending on the sensitivity of the reports they want delivered.
- ProxyExchange: Encrypts sensitive data (specific to engagements and attend meetings) using AES256 via Oracle function within the database. Personal information is only collected in the case of meeting attendance, which requires identification.
- Securities Class Action Services (SCAS): Client data is stored in one consolidated database with segregation of client data achieved through client specific encryption. ISS maintains a passphrase (using a system generated client specific Universal Unique Identifier (UUID)) protected 1024-bit asymmetric key per client. Client data is symmetrically encrypted using this

client specific key as the data is loaded into the database. As an additional contextual level of security, ISS uses a system generated row specific authenticator when the data is encrypted.

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.

9. Physical and Environmental Security

Key Points

Key areas of physical security include:

- 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.
- 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 using a pair of datacenters in the United States which provide primary and recovery services. ISS maintains a pair of European Union (EU) datacenters serving only specific client operations as designated by contractual agreements. ISS' datacenter facilities and physical security systems were designed to provide extremely hardened, state-of-the-art, secure operational locations.

US Datacenters: 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. ISS reviews the SOC1, SOC2, and SOC3 reports for Switch on an annual basis.

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 man-traps built over a fire corridor wall construction. All access points of the man-traps 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 man-trap 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.

EU Datacenters: ISS contracts with SunGard Availability Services in Europe. Both EU datacenters have completed SSAE audits, the reports of which are provided to and reviewed by ISS annually.

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 EU 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.

Office Equipment: Users must lock or logoff workstations, systems or applications before leaving unattended. Additionally, systems are configured with a technical control to terminate sessions after a pre-defined period of inactivity. Terminated or locked sessions require re-authentication prior to returning users to the previous session. ISS has implemented a “Clear Desk and Clear Screen” policy to help ensure documents, printouts, removable media or other information assets containing sensitive information are not left unattended.

10. Operations Security

Key Points

- Malware protection at multiple points:
- Endpoints: Endpoint protection covering anti-spam, phishing and malware applied throughout the organization and updated multiple times a day.
- Email Gateway: Detection files (DAT) are updated daily from vendor ensuring up-to-date protection against phishing attempts, spam/malware.
- Web Gateway: Category filtering blocks personnel from websites which are highly suspected of current or past virus activity and safeguard traffic to suspicious or scrupulous websites.
- Backup program provides encrypted backups in both the production datacenter for rapid recovery as well as the disaster recovery datacenter for continuity purposes.
- All ISS productions servers, networks and applications are monitored 24x7x365 by fully automated monitoring and alerting systems.
- Vulnerability Management Program ensures patching guidelines are established, monthly network vulnerability scans and quarterly application scans are completed as well as annual penetration and ethical hack testing is performed.

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 to a Data Domain 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 a Data Domain that has the capacity to store the backup data for a period of 7 years.

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 monthly. Results of these scans are distributed to appropriate stakeholders for remediation. An application layer vulnerability assessment is performed for ISS applications on an annual basis leveraging vulnerability and penetration testing tools. Ethical hacking by an independent third party is performed annually.

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. If an information asset owner discovers a vulnerability that was not previously identified, they should immediately contact the Service Desk to create a high priority ticket assigned to the Information Security Office.

The ISS patch cycle is determined on two criteria: criticality and OS 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. Generally, guidelines are endpoints and UAT/Prod are monthly and Dev/QA are daily.

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

11. Communications Security

Key Points

- Network: Multi-zone security architecture controlled by firewalls between tiers.
- Remote access: Remove access to the ISS network requires Cisco AnyConnect along with Okta Verify to enforce multi-factor authentication of users.
- Privilege access: All access to datacenter assets require privilege access along with multi-factor authentication.
- Microsoft Mobile Device Management software is used to secure mobile devices.
- Data Loss Prevention (DLP) key areas:

  - Proactive email review: Helps detect the presence of information commonly considered to be personally identifiable information (PII) in the United States, including information like social security numbers or driver's license numbers.
  - Reactive email review: Compliance reviews email content for key language usage and patterns for any suspicious activity.
  - Email communication: ISS supports opportunistic email encryption via TLS for the protection of email traffic. Currently TLS 1.2 is preferred, TLS 1.0/1.1 are enabled but de-prioritized.
  - Web access: Content filtering in place to prevent access to external email providers and file sharing sites from ISS systems. 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.

- Network devices: All ISS systems which can be accessed outside of an ISS facility are AES 256-bit (CBC) encrypted.
- Application access: Applications are available only via https to ensure that all application data is encrypted before transmission.
- Application reporting: User activity within ProxyExchange monitored for anomalies (increased report downloads, printing, etc.) for action.
- Removable media: 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. If USB devices are used, they are wholly encrypted and only available for use on another ISS-protected machine. Once encrypted, USB devices are unreadable from home PCs or any non-ISS device.

ISS has a global MPLS network that connects the global offices in a secure, private network. Endpoints are continuously monitored. Additional network security controls include:

- A multi-zone security architecture that helps ensure 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 and reviewed and approved prior to implementation.
- Firewalls allow only the network traffic necessary for the applications to operate and be managed.
- Administrative access to network devices is strictly limited to authorized IT personnel.

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.

Remote Working/Secure VPN: ISS provides Virtual Private Network (VPN) access for select employees that may require this type of access to support their job role. VPN devices are utilized at ingress and egress points to the global Wide Area Network (WAN). Two-factor authentication is required for remote VPN access. ISS supports remote working capabilities where appropriate for its staff. Additional controls and

guidance for staff working remotely include but are not limited to:

- Training and education on remote working risk which must be completed before remote access is provided;
- Full disk encryption on laptops;
- Secure mobility clients on laptops enforcing VPN use;
- Microsoft Mobile Device Management (MDM) software is used to provision and secure ‘Bring Your Own Device’ mobile devices.
- Approved personal devices may access ISS email functionality using the Outlook Web Access (OWA) through mobile browser and Outlook Application.

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.

Data Loss Prevention: Data Loss Prevention (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.

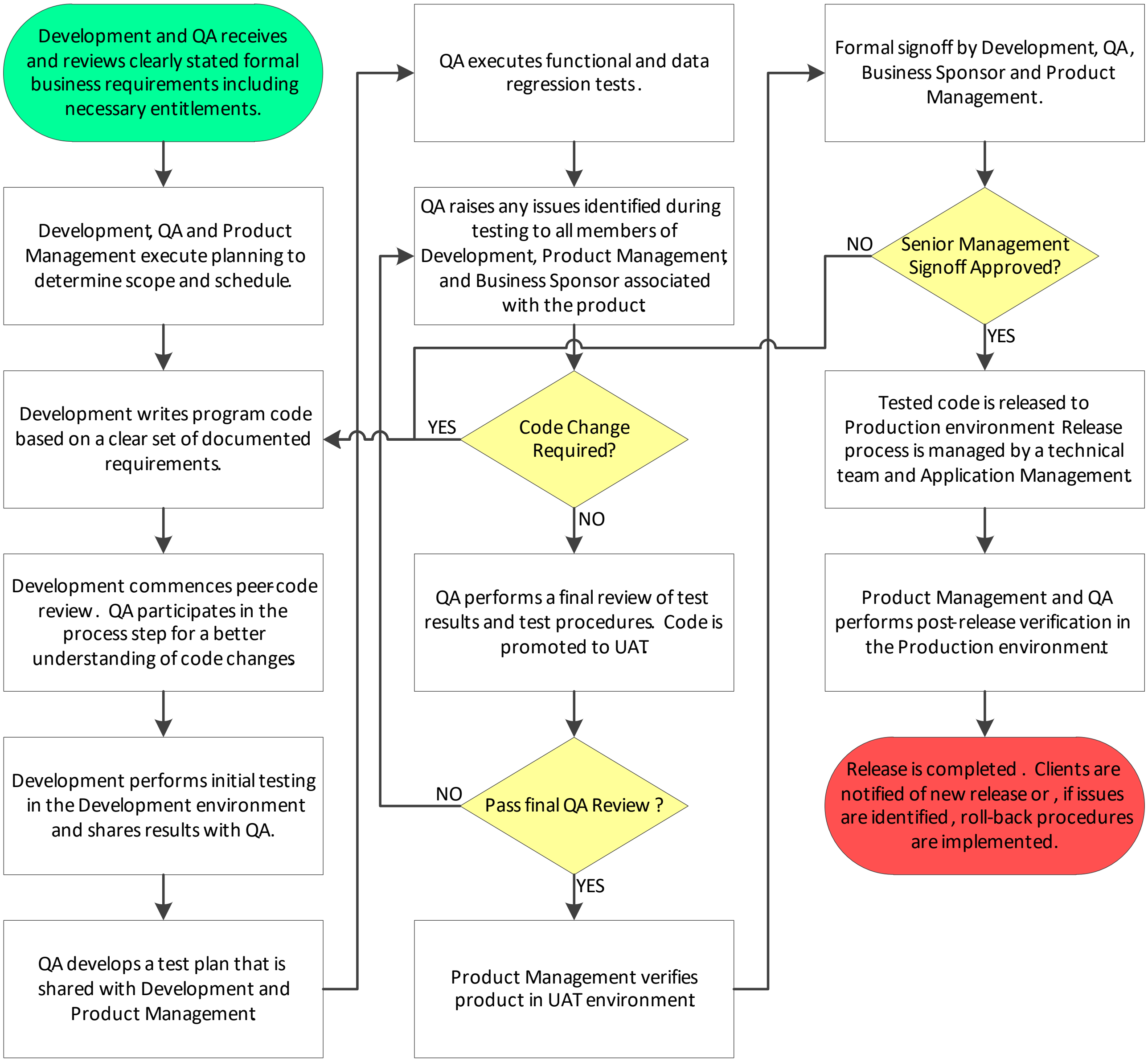
12. System Acquisition, Development and Maintenance

Key Points

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

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.


Development and QA receives and reviews clearly stated formal business requirements including necessary entitlements.
Development, QA and Product Management execute planning to determine scope and schedule.
Development writes program code based on a clear set of documented requirements.
Development commences peer code review. QA participates in the process step for a better understanding of code changes
Development performs initial testing in the Development environment and shares results with QA.
QA develops a test plan that is shared with Development and Product Management
QA executes functional and data regression tests.
QA raises any issues identified during testing to all members of Development, Product Management, and Business Sponsor associated with the product
YES
Code Change Required?
NO
QA performs a final review of test results and test procedures. Code is promoted to UAT
NO
Pass final QA Review ?
YES
Product Management verifies product in UAT environment
Formal signoff by Development, QA, Business Sponsor and Product Management.
NO
Senior Management Signoff Approved?
YES
Tested code is released to Production environment. Release process is managed by a technical team and Application Management
Product Management and QA performs post-release verification in the Production environment
Release is completed. Clients are notified of new release or, if issues are identified, roll-back procedures are implemented.

13. Third-Party Provider Relationships

A Third-Party Provider risk management program is in place to minimize risk that may be experienced by engaging a third-party provider. Third parties are tiered, based on risk, using various risk-related criteria. Depending on the risk score, various methods are used to evaluate third-party providers, including a combination of reviews of the third party'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 the clients.

14. Incident Management

ISS maintains an Information Security Incident Response Policy that requires incidents to be reported, acted upon, escalated, and resolved in a timely, repeatable and reliable manner. To help 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.

15. Independent Review

ISS undergoes an SSAE audit on an annual basis that is performed by an independent third party. This is a detailed and comprehensive audit and the annual SSAE report is available to clients upon request through the Client Services team. The annual SSAE audit consists of 50 activities in five key control areas:

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

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. CYBERSECURITY MANAGEMENT & DEFENSE SYSTEM (CMDS)

Key Points

Key tools and technologies include, but are not limited to, the following:

- Complete Data Protection Suite (ePO):
- Endpoint security (anti-malware and anti-spam)
- Endpoint encryption
- Removable media control
- Data loss prevention controls
- Email Gateway:
- Anti-malware and anti-spam protection
- Whitelist/Blacklist functionality
- Data loss prevention controls
- Email O365 Security and Compliance Center
- Compliance email and instant message archival
- Threat management depth
- Data loss prevention controls
- Web Gateway:
- Network web protection
- Permitted categories
- Data loss prevention controls
- Enterprise Security Manager (SIEM):
- Real-time visibility into activity on systems, networks, databases and applications.
- Alerts and Reports
- Data loss prevention controls
- 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.

Based on the Securities and Exchange Commission (SEC) Office of Compliance Inspections and Examinations (OCIE), guidance ISS has leveraged existing controls and implemented ancillary controls that work in concert to support the Cybersecurity Management and Defense System (CMDS). This section contains an overview of the CMDS.

In addition to the comprehensive control framework in place, ISS has made a significant investment in security tools and technologies and implemented a variety of suites in support of the information security and cybersecurity programs. While specific details about settings and configurations are classified as *Confidential*, we have included an overview of several of the tools deployed throughout the enterprise in this section for your reference.

1. Security Tools

Key Points

Data Loss Prevention (DLP) Key Areas (not all inclusive):

- Host and network DLP
- Proactive Email Review - Helps detect the presence of information commonly considered to be personally identifiable information (PII) in the United States, including information like social security numbers or driver's license numbers.
- Reactive Email Review - Compliance reviews email content for key language usage and patterns for any suspicious activity.
- Email Communication – ISS supports opportunistic email encryption via TLS for the protection of email traffic. Currently TLS 1.2 is preferred, TLS 1.0/1.1 are enabled but de-prioritized.
- Web Review - Content filtering in place to prevent access to external email providers and file sharing sites from ISS systems. 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.
- Network - All ISS systems which can be accessed outside of an ISS facility are AES 256-bit (CBC) encrypted.
- Application Access - Access is available only via https to ensure that all application data is encrypted before transmission.
- Application Reporting - User activity within ProxyExchange monitored for anomalies (increased report downloads, printing, etc.) for action.
- Removable Media - 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. If USB devices are used, they are wholly encrypted and only available for use on another ISS-protected machine. Once encrypted, USB devices are unreadable from home PCs or any non-ISS device.

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 antimalware, 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 help 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.
- Helps to 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 help 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. 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.

4. BUSINESS CONTINTUITY MANAGEMENT SYSTEM (BCMS)

Key Points

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.

- ISS consists of 30 global office locations with the ability to transfer work processes from 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.
- With global office locations, if loss of access is an isolated event, work transfer would be a solution for ISS. Other solutions noted include backup restore full or local dependent on situation.
- ISS maintains a disaster recovery datacenter which could be initialized if a DR event was declared.
- ISS maintains a work remote/work from home strategy for personnel for isolated business continuity events. With global office locations, ISS can rely on other office locations as needed.
- Crisis management teams are defined for each office location, typically including at minimum the Head of Office, Office Manager, and 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.

1. Business Impact Analysis

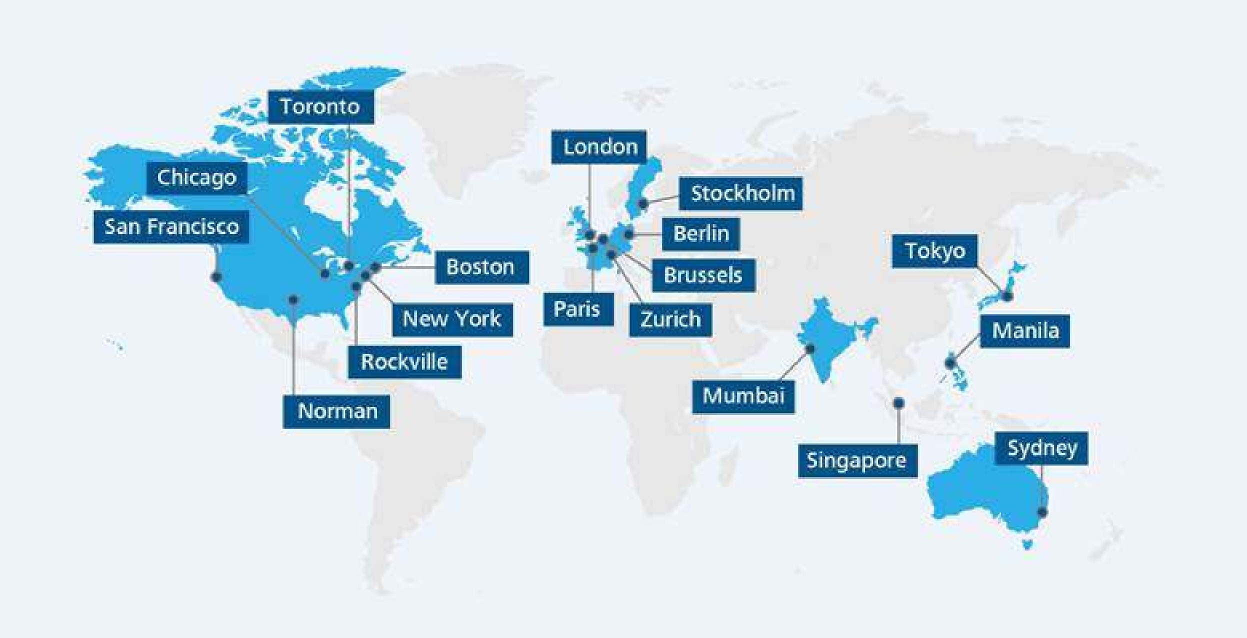
Business Impact Analysis (BIA) is the method by which business activities can be prioritized based on criticality. A BIA determines levels of criticality, risks, and operational requirements needed to provide critical products and services. A BIA has been completed for each critical operational function 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.

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 Information
- Local IT Information
- Business Impact Analysis
- Recovery Objectives
- Business Continuity Plan
- References
- BCP Run Book

The ISS business maintains proxy voting and transaction operations in London, UK; Manila, Philippines; Tokyo, Japan; Norman, Oklahoma, USA; and Rockville, Maryland, USA. The London office primarily serves the European Market. Tokyo and Manila serve the Asia market. Norman and Rockville offices serve the North America market.



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 can 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.

ISS performs annual Disaster Recovery testing. Once invoked, the Disaster Recovery objectives are as follows:

- The Recovery Time Objective (RTO) for client-facing applications is one calendar day.
- The Recovery Point Objective (RPO) for client-facing applications is one business day.

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 in the disaster recovery site within 24 hours.

3. 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 a significant 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.

4. 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 performed:

- Reinforce and add to existing healthy habits already published.
- Communicate policy on self-isolation if an employee or family member does not feel well.
- HR policy review or policy adjustments for 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.
- Travel Policy: Reference recommendations from authorities such as the CDC, WHO and the State Department. Leave decision to travel up to employees and their managers. No forced travel.
- Vaccinations: Employees should go through normal healthcare providers for vaccinations.

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 for the next 6 months, 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 for the next 3 months.
- Business leaders will be responsible for reviewing scenarios and advising on potential business impacts.

Communications. As with all major events, communication is key during a Pandemic event. To support continued communications, ISS has recorded the following 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 Pandemic event.
- Verify Vertical Response system is ready for a mass-client email, if deemed to be necessary.
- Provide additional communications to clients and shareholders if the pandemic situation escalates.

5. 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 help 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 help ensure ISS can sustain operational and support capabilities in the event of an unplanned, extended outage.

6. 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 the ProxyExchange and SCAS applications.
- Testing remote continuity planning, VPN availability and stability for various office locations.
- Office generator load testing.
- Failover and failback of databases to the disaster recovery datacenter.
- Tests were completed successfully with no significant remediation items to complete.

Lessons learned are tracked through the testing report as well as the central change management system, JIRA. Tests were completed successfully with no significant remediation items to complete.

5. APPENDIX A: INFORMATION SECURITY POLICIES

ISS is frequently asked to provide copies of the Information Security Policies. The Information Security Policies are classified as Internal Use Only and are not available for external distribution. Understanding the needs of the clients to meet internal information security and regulatory compliance initiatives when it comes to due diligence, this Appendix was developed, which contains the tables of content for each of the information security policies.

01: Information Security Policies – 1.7, Dated 07/18/2018 Version 1.7, Dated 07/18/2018
1. Purpose 2. Scope 3. Information Security Management System (ISMS) 3.1. ISMS Objectives 3.2. Framework of Controls 4. Requirements 4.1. Management Direction for Information Security 4.1.1.Information Security Policies 4.1.2.Review of Information Security Policies 4.2. Responsibilities 5. Compliance 6. References
02: Organization of Information Security – Version 1.7, Dated 07/18/2018 1.7, Dated 07/18/2018
1. Purpose 2. Scope 3. Requirements 3.1. Internal Organization 3.1.1.Information Security Roles and Responsibilities 3.1.2.Segregation of Duties 3.1.3.Contact with Authorities 3.1.4.Contact with Special Interest Groups 3.1.5.Information Security in Project Management 3.2. Mobile Device and Teleworking 3.2.1.Mobile Device Policy 3.2.2.Teleworking 4. Compliance 5. References
03: Personnel Security – Version 1.7, Dated 07/18/2018
1. Purpose 2. Scope 3. Requirements 3.1. Prior to Employment 3.1.1.Screening 3.1.2.Terms and Conditions of Employment 3.2. During Employment 3.2.1.Management Responsibilities 3.2.2.Information Security Awareness Training 3.2.3.Disciplinary Process

3.3. Termination or Change of Employment
3.3.1.Termination or Employment Change Responsibilities
4. Compliance
5. References

04: Information Asset Management – Version 1.7, Dated 07/18/2018

1. Purpose
2. Scope
3. Requirements
3.1. Responsibility for Information Assets
3.1.1.Inventory of Assets
3.1.2.Ownership of Assets
3.1.3.Acceptable Use of Assets
3.1.4.Return of Assets
3.2. Information Classification
3.2.1.Classifying Information Assets
3.2.2.Labeling Information Assets
3.2.3.Handling Information Assets
3.3. Media Handling
3.3.1.Management of Removable Media
3.3.2.Disposal of Media
3.3.3.Physical Media Transfer
4. Compliance
5. References

05: Access Control – Version 1.7, Dated 07/18/2018

1. Purpose
2. Scope
3. Requirements
3.1. Business Requirements for Access Control
3.1.1.Access Control Policy
3.1.2.Access to Networks and Network Services
3.2. User Access Management
3.2.1.User Provisioning and De-Provisioning
3.2.2.User Access Provisioning
3.2.3.Management of Privileged Access Rights
3.2.4.Management of Secret Authentication Information of Users
3.2.5.Review of User Access Rights
3.2.6.Removal or Adjustment of Access Rights
3.3. User Responsibilities
3.3.1.Use of Secret Authentication Information
3.4. System and Application Access Controls
3.4.1.Information Access Restriction
3.4.2.Secure Logon Procedures
3.4.3.Password Management System
3.4.4.Use of Privileged Utility Programs
3.4.5.Access Control to Program Source Code
4. Compliance

3.3.2.Backup Controls and Requirements 3.3.3.Backup Media Leaving ISS Facilities 3.4. Logging and Monitoring 3.4.1.Event Logging 3.4.2.Protection of Log Information 3.4.3.Administrator and Operator Logs 3.4.4.Clock Synchronization 3.5. Control of Operational Software 3.5.1.Installation of Software on Operational Systems 3.6. Technical Vulnerability Management 3.6.1.Managing Vulnerabilities 3.6.2.Restrictions on Software Installations 3.7. Information Systems Audit Considerations 3.7.1.Information Systems Audit Controls 4. Compliance 5. References
09: Communications Security – Version 1.7, Dated 07/18/2018
1. Purpose 2. Scope 3. Requirements 3.1. Network Security Management 3.1.1.Network Controls 3.1.2.Segregation of Network Services 3.1.3.Segregation in Networks 3.2. Information Transfer 3.2.1.Information transfer Policies and Procedures 3.2.2.Agreement on Information Transfer 3.2.3.Electronic Messaging 3.2.4.Confidentiality/Non-Disclosure Agreements 4. Compliance 5. References
10: System Acquisition, Development and Maintenance – Version 1.7, Dated 07/18/2018
1. Purpose 2. Scope 3. Requirements 3.1. Security Requirements for Information Systems 3.1.1.Information Security Requirements Analysis and Specification 3.1.2.Securing Application Services on Public Networks 3.1.3.Protecting Application Services Transactions 3.2. Security in Development and Support Processes 3.2.1.Secure Development Policy 3.2.2.System Change Control Procedures 3.2.3.Technical Review of Applications after Changes 3.2.4.Restrictions of Changes to Software Packages 3.2.5.Secure System Engineering Principles 3.2.6.Secure Development Environment 3.2.7.Outsourced Development

3.2.8.System Security Testing
3.2.9.System Acceptance Testing
3.3. Test Data
3.3.1.Protection of Test Data
4. Compliance
5. References

11: Third-Party Provider Relationships – Version 1.7, Dated 07/18/2018

1. Purpose
2. Scope
3. Requirements
3.1. Information Security in Supplier Relationships
3.1.1.Information Security Policy for Supplier Relationships
3.1.2.Addressing Security with Supplier Agreements
3.1.3.Information and Communication Technology Supply Chain
3.2. Supplier Service Delivery Management
3.2.1.Monitoring and Review of Supplier Services
3.2.2.Managing Changes to Supplier Services
4. Compliance
5. References

12: Information Security Incident Management – Version 1.7, Dated 07/18/2018

1. Purpose
2. Scope
3. Terms and Definitions
4. Requirements
4.1. Management of Information Security Incidents and Improvements
4.1.1.Responsibilities and Procedures
4.1.2.Reporting Information Security Events
4.1.3.Reporting Information Security Weaknesses
4.1.4.Assessment of and Decisions on Information Security Events
4.1.5.Response to Information Security Incidents
4.1.6.Learning from Information Security Incidents
4.1.7.Collection of Evidence
5. Compliance
6. References

13: Business Continuity Management – Version 1.7, Dated 07/18/2018

1. Purpose
2. Scope
3. Requirements
3.1. Business Continuity Plan (BCP)
3.1.1.Business Impact Analysis and Risk Assessments
3.1.2.Developing and Implementing Continuity Plans
3.1.3.Business Continuity Framework
3.1.4.Testing, Maintaining and Reassessing Business Continuity Plans
3.2. Information Security Continuity
3.2.1.Planning Information Security Continuity
3.2.2.Implementing Information Security Continuity
3.2.3.Verifying, Reviewing and Evaluating Information Security Continuity

3.3. Redundancies
3.3.1.Availability of Information Processing Facilities
4. Compliance
5. References
14: Compliance – Version 1.7, Dated 07/18/2018
1. Purpose
2. Scope
3. Requirements
3.1. Compliance with Legal and Contractual Requirements
3.1.1.Identification of Applicable Legislation and Contractual Requirements
3.1.2.Intellectual Property Rights
3.1.3.Protection of Records
3.1.4.Privacy and Protection of Personally Identifiable Information
3.1.5.Regulation of Cryptographic Controls
3.2. Information Security Reviews
3.2.1.Independent Review of Information Security
3.2.2.Compliance with Security Policies and Standards
3.2.3.Technical Compliance Review
4. Compliance with Information Security Controls

6. APPENDIX B: INFORMATION SECURITY STANDARDS

ISS is frequently asked to provide copies of the Information Security Standards. The Information Security Standards are classified as *Internal Use Only* and are not available for external distribution. Understanding the needs of the clients to meet internal information security and regulatory compliance initiatives when it comes to due diligence, this Appendix was developed, which contains the tables of content for each of the information security standards.

01: Risk Management – Version 1.7, Dated 07/18/2018
1. Purpose
2. Scope
3. Requirements
3.1. Team Establishment
3.2. Scope of Risk Assessments
3.3. Identification of Assets for Review
3.4. Operational Importance of Assets being Evaluated
3.5. Threats and Vulnerability Identification and Evaluation
3.6. Risk Ratings for Reviewed Assets
3.7. Developing and Updating the Risk Remediation Plan
4. Compliance
5. References
02: Information Protection – Version 1.7, Dated 07/18/2018
1. Purpose
2. Scope
3. Requirements
3.1. Information Asset Classification

3.1.1.Tier 1 – Public
3.1.2.Tier 2 – Internal Use Only
3.1.3.Tier 3 – Confidential
3.1.4.Tier 4 – Restricted
3.1.5.Classification Review and Maintenance
3.2. Information Handling
3.2.1.Storage Requirements
3.2.2.Transmission and Distribution Requirements
3.2.3.Physical Security Requirements
3.2.4.Destruction, Disposal, Recycle and Reuse Requirements
3.2.5.Duplication Requirements
3.2.6.Security Logging, Monitoring and Auditing Requirements
4. Compliance
5. References

03: Data Privacy – Version 1.7, Dated 07/18/2018

1. Purpose
2. Scope
3. Requirements
3.1. Accountability
3.2. Review
3.3. Regulatory Requirements
3.4. Communication and Training
3.4.1.External Communications – Website Privacy Statement
3.4.2.Client Communications – Provided Services
3.4.3.Internal Communications
3.4.4.Training
3.5. Third-Party Providers
3.5.1.Contractual Requirements
3.5.2.Due Diligence
3.6. Privacy Incident Management
3.7. Managing International Privacy Information
4. Compliance
5. References

04: Account and Password Management – Version 1.7, Dated 07/18/2018

1. Purpose
2. Scope
3. Requirements
3.1. Account User ID Standard
3.2. Standard User Accounts
3.3. Privileged User Accounts
3.4. Training Accounts
3.5. System Accounts
3.6. Service Accounts
3.7. Employee User IDs
3.8. Non-Employee User IDs
3.9. General or Generic Accounts
3.10. Authentication Requirements

3.11. Failed Logon Attempts
3.12. Inactive Accounts
3.13. Idle Session Timeout
3.14. Last Logon and Logoff
3.15. Job, Role or Function Changes
3.16. Extended User Absences
3.17. Terminations
3.18. Issuing and Changing Passwords
3.19. Password Complexity
3.20. Password Confidentiality
3.21. Password Resets
3.22. Password Expiration
3.23. General Password Guidelines
3.24. Account Audits
4. Compliance
5. References

05: Email Security – Version 1.7, Dated 07/18/2018

1. Purpose
2. Scope
3. Requirements
3.1. General Use of Email Systems
3.2. Email Account Standards
3.3. Expectation of Privacy
3.4. Information Protection
3.5. Shared Email Access
3.6. Email Attachments and Signatures
3.7. Email Retention
3.8. Email Storage Requirements
3.9. Mailbox Deletion
3.10. Mass Mailings
3.11. Security Settings
3.12. Periodic Review of Authorized Accounts
3.13. Virus Protection
3.14. Reporting Security Problems
4. Compliance
5. References

06: Internet and Intranet Security – Version 1.7, Dated 07/18/2018

1. Purpose
2. Scope
3. Requirements
3.1. General Use of Internet and Intranet Resources
3.2. Posting Information
3.3. Information Protection
3.4. Expectation of Privacy
3.5. Proprietary Information
3.6. Personal Use of the Internet
3.7. Public Representations

3.8. Reporting Security Problems 3.9. Audit and Accountability of Internet Connections 4. Compliance 5. References
07: Remote Access – Version 1.7, Dated 07/18/2018
1. Purpose 2. Scope 3. Requirements 3.1. General Remote Access Standards 3.2. Access Requests and Approvals 3.3. Remote Access Software 3.4. Remote User Authentication 3.5. Account Requirements 3.6. Physical Security of Remote User Systems 3.7. Remote Access Configuration Information 3.8. Remote Administration of Information Assets 3.9. Remote Access to Gateways between Networks 3.10. Token Inventory 4. Compliance 5. References
08: Software Security – Version 1.7, Dated 07/18/2018
1. Purpose 2. Scope 3. Requirements 3.1. Purchase of Software 3.2. Software Registration 3.3. Software Installation Guidelines 3.4. Freeware, Shareware and Evaluation Software 3.5. Auditing, Monitoring and Reconciliation 4. Compliance 5. References
09: ISS and BYOD Mobile Device Security – Version 1.7, Dated 07/18/2018
1. Purpose 2. Scope 3. Requirements 3.1. ISS Mobile Device Requirements 3.2. BYOD Acceptable Use 3.3. BYOD Devices and Support 3.4. BYOD Security 3.5. BYOD Risk, Liabilities and Disclaimers 4. Compliance 5. References
10: Visitor Security Version 1.7, Dated 07/18/2018
1. Purpose 2. Scope 3. Exclusions 4. Requirements

14: System and Application Security – Version 1.7, Dated 07/18/2018

5.11. Passwords in Audit Logs
5.12. Privacy Policy
5.13. URL Composition
5.14. Cookie Security
5.15. Parameter Checking
5.16. Page Caching
5.17. Sanitization of Browser Input
5.18. The Use of POST versus GET
5.19. Absolute Path and File Names
5.20. Use of Production Data

6. Testing and Quality Assurance
    6.1. Security Components Testing Procedures
    6.2. Pre-Production Accounts
    6.3. Default Access Rights
    6.4. Source Code Information
    6.5. System Cleanup
    6.6. Test and QA Environments
7. Production
    7.1. Removal of Unnecessary Services
    7.2. Performance Planning
    7.3. Patches and Updates
    7.4. Software Scanning
    7.5. Removal of Default Accounts
    7.6. System and Application Reviews
    7.7. Offline Storage Security
    7.8. Process for Granting Information Access
    7.9. Account Termination or Transfer
    7.10. Background Processes
    7.11. Application Source Code Security
    7.12. Console Security
    7.13. Operating System Security Configuration Standards
    7.14. Management of Audit Logs
    7.15. Inactive Accounts
8. Compliance
9. References

15: Network Security Baseline – Version 1.7, Dated 07/18/2018

1. Purpose
2. Scope
3. Network Management Standards
    3.1. Network Documentation
    3.2. Network Segmentation
    3.3. Service Isolation
    3.4. Physical Security
    3.5. IP Address Scheme
    3.6. Private Address Scheme
    3.7. Device Naming Convention
    3.8. Redundancy

16: Cloud Computing – Version 1.7, Dated 07/18/2018

17: Computing Platform – Version 1.7, Dated 07/18/2018

4.1.5.Logging
4.1.6.Workstation Naming
4.1.7.Workstation Changes
4.1.8.Workstation Integrity
4.1.9.Functionality
4.2. Account Requirements
4.2.1.Maintenance Accounts
4.2.2.Default Accounts
4.2.3.User Accounts
4.2.4.System IDs
4.2.5.Administrative Accounts
4.2.6.Anonymous Accounts
4.2.7.Audit Accounts
4.3. Account Management
4.4. Protection Requirements
4.4.1.Authorization
4.4.2.Authentication
4.4.3.Accountability
4.4.4.Foreign Systems
5. Platform Management
5.1. Baseline
5.2. Monitor
5.3. Manage
5.4. Audit
6. Exceptions
6.1. Authorizations
7. Maintenance and Review

7. APPENDIX C: INCIDENT RESPONSE PLAN SUMMARY

ISS is frequently asked to provide copies of the Incident Response Plan (IRP). The IRP is classified as *Internal Use Only* and not available for external distribution. Understanding the needs of the clients to meet internal information security and regulatory compliance initiatives when it comes to due diligence, this Appendix was developed, which contains the tables of content for the IRP.

Incident Response Plan – Version 1.7, Dated 07/18/2018
1. Purpose 2. Scope 3. Plan Overview 3.1. Incident Response Charter 3.2. Intended Audience 3.3. Assumptions 3.4. Enforcement 3.5. Deviations 4. Definition, Identification and Declaration 4.1. Definition

DATA. ANALYTICS. INSIGHT

Environmental. Social. Governance.

GET STARTED WITH ISS SOLUTIONS

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

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.