

Standardized Information Gathering (SIG) Lite Questionnaire

1. Business Information

1.1 Assessee Name*

1.2 Assessee Job Title*

1.3 Assessee Contact Information*

1.4 Names and titles/functions of individuals who contributed to this questionnaire*

1.5 Date of Response*

1.6 Name of the holding or parent company*

1.7 Company/business name*

1.8 Publicly or privately held company*

1.9 If public, what is the name of the Exchange?*

1.10 If public, what is the trading symbol?*

1.11 Type of legal entity and state of incorporation*

1.12 How long has the company been in business?*

1.13 Are there any material claims or judgments against the company?*

1.14 If yes, describe the impact it may have on the services in scope of this document*

1.15 Has your company suffered a data loss or security breach within the last 3 years?*

1.16 If yes, please describe the loss or breach*

1.17 Has any of your Third Party Vendors suffered a data loss or security breach within the last 3 years?*

1.18 If yes, please describe the loss or breach*

1.19 Are the answers in this questionnaire for only one facility or geographic location? If yes, provide description of physical location (address, city, state, country)*

1.20 Backup site physical address*

1.21 Any additional locations where Scoped Systems and Data is stored*

1.22 If yes, provide each location (address, city, state, country)*

1.23 Are the answers to this questionnaire for only one specific type of service? If yes, describe the service*

1.24 Are software applications provided?*

1.25 List the applications provided that are in scope*

1.26 Identify the applications which are covered by the secure software development lifecycle*

1.27 What type of software is being provided, select all that apply

1.27.1 Commercial Off-The-Shelf (COTS)*

1.27.2 Custom Developed*

1.27.3 Cloud*

1.27.4 Mobile*

1.27.5 Open Source Software*

1.27.6 Other*

2. Documentation

2.1 Information Security policies and procedures. This should include the following (if not, provide the individual documents as necessary): a) Hiring policies and practices and employment application, b) User Account administration policy and procedures for all supported platforms where Scoped Systems and Data are processed and network/LAN access, c) Supporting documentation to indicate completion of User Entitlement reviews, d) Employee Non-disclosure agreement document, e) Information Security Incident Report policy and procedures, including all contract information, f) Copy of Visitor policy and procedures, g) Security Log Review policies and procedures, h) Copy of third party risk management policies and procedures*

2.2 Copy of internal or external information security audit report*

2.3 Information technology and security organization charts (including where Respondent information security resides and the composition of any information security steering committees). Note: Actual names of employees are not required*

2.4 Physical Security policy and procedures (building and/or restricted access)*

2.5 Third party security reviews/assessments/penetration tests*

2.6 Legal clauses and confidentiality templates for third parties*

2.7 Topics covered in the security training program*

2.8 Security incident handling and reporting process*

2.9 Network configuration diagrams for internal and external networks defined in scope. Note: Sanitized versions of the network diagram are acceptable*

2.10 System and network configuration standards*

2.11 System backup policy and procedures*

2.12 Offsite storage policy and procedures*

2.13 Vulnerability and threat management scan policy and procedures*

2.14 Application security policy*

2.15 Change control policy/procedures*

2.16 Problem management policy/procedures*

2.17 Certification of proprietary encryption algorithms*

2.18 Internal vulnerability assessments of systems, applications, and networks*

2.19 Software development and lifecycle (SDLC) process document*

2.20 Business Resiliency (continuity plan) (BCP) and/or Disaster Recovery Plan*

2.21 Most recent BCP/DR test dates and results*

2.22 Most recent AUP/SSAE16/SOC2 audit report(s)*

2.23 Privacy Policies (internal, external, web)*

2.24 Executive Summary of certificates held. (e.g. PCI, HIPAA, ISO)*

2.25 Performance Reports against contracted SLAs*

3. Risk Assessment and Treatment

- 3.1 Is there a risk assessment program that has been approved by management, communicated to constituents and an owner to maintain and review the program? if yes, does it include:***
- 3.1.1 Is there a program to manage the treatment of risks identified during assessments?***
 - 3.1.2 A formal process for assigning appropriate management ownership for each risk?***
 - 3.1.3 A formal process for appropriate management knowingly and objectively accepting risks and approving action plans?***
 - 3.1.4 A formal process for tracking the status of action plans and reporting them to management?***
 - 3.1.5 Controls identified for each material risk?***
 - 3.1.6 Measures for defining, monitoring, and reporting risk metrics?***
- 3.2 Do Subcontractors have access to Scoped Systems and Data? (backup vendors, service providers, equipment support maintenance, software maintenance vendors, data recovery vendors, etc.)?***
- 3.3 A documented vendor management process in place for the selection, oversight and risk assessment of third party vendors? If yes, does it include:***
- 3.3.1 Approval by management?***
 - 3.3.2 Annual review?***
 - 3.3.3 Required reassessment when service delivery or contract changes?***
 - 3.3.4 Review of the subcontractor's vendor management policy and procedures?***

- 3.3.5 Is there a process to identify and log subcontractor information security, privacy and/or data breach issues?***
- 3.4 Is there a vendor management program?***
- 3.5 Do external parties have access to Scoped Systems and Data or processing facilities?***
- 3.6 Is the maturity of IT management processes formally evaluated at least annually using an established benchmark (e.g., COBIT maturity models)?***
- 3.7 Are there regular privacy risk assessments conducted? If yes, provide frequency and scope. If no, explain reason.***
- 3.8 Are identified privacy risks and associated mitigation plans formally documented and reviewed by management?***
- 3.9 Are reasonable resources (in time and money) allocated to mitigating identified privacy risks?***
- 3.10 Is there a compliance risk management system that addresses the quality and accuracy of reported consumer data?***
- 3.11 Is there a compliance risk management system that addresses the quality of assembling and maintaining the data?***

4. Security Policy

4.1 Is there an information security policy that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?*

4.2 Have the policies been reviewed in the last 12 months?*

5. Organizational Security

5.1 Is there a respondent information security function responsible for security initiatives?*

6. Asset and Information Management

6.1 Is there an asset management policy approved by management, communicated to constituents and an owner to maintain and review?*

6.2 Is information classified?*

6.3 Is there a removable media policy or program (CDs, DVDs, tapes, disk drives) that has been approved by management, communicated to appropriate constituents, and an owner to maintain and review the policy?*

6.4 Is Scoped Data sent or received via physical media?*

6.5 Are encryption tools managed and maintained for Scoped Data? If yes:*

6.5.1 Are clients provided with the ability to generate a unique encryption key?*

6.5.2 Are clients provided with the ability to rotate their encryption key on a scheduled basis?*

6.6 Are staff able to access client Scoped Data in an unencrypted state?*

6.7 Are staff able to access client's encryption keys?*

6.8 Is data segmentation and separation capability between clients provided?*

6.9 Does the ability exist to legally demonstrate sufficient data segmentation, in the event of a client subpoena or a forensics incident, so as not to impact other clients data if using resource pooling?*

6.10 Is there a data classification retention program that identifies the data types that require additional management and governance?*

6.11 Is there a self-service portal or API call available to clients which provides the ability to place a 'Legal hold' on client data which may be subject to a legal action, without impacting other clients data retention or destruction schedules?*

7. Human Resource Security

7.1 Is there a Human Resource policy approved by management, communicated to constituents and an owner to maintain and review? If yes, does it include:*

7.1.1 Security roles and responsibilities?*

7.1.2 Background screening?*

7.1.3 Employment agreements?*

7.1.4 Security awareness training?*

7.1.5 Disciplinary process for non-compliance?*

7.1.6 Termination or change of status process?*

7.2 Are background checks performed for Service Provider Contractors and Subcontractors?*

7.3 Do information security personnel have professional security certifications?*

8. Physical and Environmental Security

8.1 Is there a physical security program?*

8.2 Are physical security and environmental controls in the data center and office buildings?*

8.3 Are visitors permitted in the facility?*

9. Operations Management

9.1 Are management approved operating procedures utilized?*

9.2 Is there an operational change management/change control policy or program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?*

9.3 Are backups of Scoped Systems and Data performed?*

9.4 Are Cloud Services provided? If yes, what service model is provided (select all that apply):*

9.4.1 Software as a Service (SaaS)?*

9.4.2 Infrastructure as a Service (IaaS)?*

9.4.3 Private cloud?*

9.4.4 Public cloud?*

9.4.5 Community cloud?*

9.4.6 Hybrid cloud?*

9.5 Is there a client management portal which allows distributed business accounts (business units/departments) to be managed under a single central corporate account?*

9.6 Are application self service features or an Internet accessible self-service portal available to clients?*

9.7 Can clients run their own security services within their own cloud environment?*

9.8 Is there a management approved process to ensure that image snapshots containing Scoped Data are authorized prior to being snapped?*

- 9.9 Is there a formal process to ensure clients are notified prior to changes being made which may impact their service? If yes, what is the communication method:*
- 9.10 Is there a scheduled maintenance window? If yes, what is the frequency:*
- 9.11 Is there a scheduled maintenance window which results in client downtime? If yes, what is the downtime:*
- 9.12 Is there an online incident response status portal, which outlines planned and unplanned outages? If yes, how long after an unplanned outage is this updated:*

10. Access Control

10.1 Are electronic systems used to transmit, process or store Scoped Systems and Data?*

10.2 Are individual IDs required for user authentication to applications, operating systems, databases and network devices?*

10.3 Are passwords used?*

10.4 Is there a password policy for systems that transmit, process or store Scoped Systems and Data that has been approved by management, communicated to constituents, and enforced on all platforms?*

10.5 Is remote access permitted?*

10.6 Is standards based federated ID capability available to clients (e.g., SAML, OpenID)?*

10.7 Is two factor authentication required to access the production environment containing Scoped Data?*

10.8 Are staff able to access client Scoped Data? If not, please identify the controls used to prevent this?*

10.9 Is there a process which allows the client to specifically list who from the provider will have access to their Scoped Systems and Data?*

11. Application Security

11.1 Are applications used to transmit, process or store Scoped Data?*

11.2 Is a web site supported, hosted or maintained that has access to Scoped Systems and Data?*

11.3 Are Web Servers used for transmitting, processing or storing Scoped Data? If yes, for all server platforms is/are:*

11.3.1 Is HTTPS enabled for all web pages used as part of the scoped service?*

11.3.2 All available high-risk security patches applied and verified at least monthly?*

11.3.3 Are third party alert services used to keep up to date with the latest vulnerabilities?*

11.3.4 Events relevant to supporting incident investigation regularly reviewed using a specific methodology to uncover potential incidents?*

11.3.5 Operating system and application logs relevant to supporting incident investigation protected against modification, deletion, and/or inappropriate access?*

11.4 Is application development performed?*

11.4.1 Is there a secure software development lifecycle policy (including mobile software applications) that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?*

11.4.2 Is development, test, and staging environment separate from the production environment? If so, how are they segmented:*

11.4.3 Is there a formal Software Development Life Cycle (SDLC) process?*

11.4.4 Are change control procedures required for all changes to the production environment?*

11.4.5 Is Scoped Systems and Data ever used in the test, development, or QA environments?*

11.4.6 Is there a documented change management / change control process?*

11.4.7 Are compilers, editors or other development tools present in the production environment?*

11.4.8 Is a secure code review performed at least annually?*

11.4.9 Is each release subject to a full secure code review?*

11.5 Are applications analyzed on a regular basis to determine their vulnerability against recent attacks?*

11.6 Is there a formal development methodology in operation? If yes, which groups does it include?:*

11.7 Are mobile applications that access Scoped Systems and Data developed?*

12. Incident Event and Communications Management

12.1 Is there an Incident Management Program that has been approved by management, communicated to constituents and an owner to maintain and review the program? If yes, does the program include:

*

12.1.1 Privacy Incidents?*

12.2 Is there a formal Incident Response Plan?*

12.3 Is there a 24x7x365 staffed phone number available to clients to report security incidents?*

13. Business Resiliency

- 13.1 Is there an established Business Resiliency program that has been approved by management and communicated to appropriate constituents?*
- 13.2 Has a Business Impact Analysis been conducted?*
- 13.3 Is there a formal process focused on identifying and addressing risks of disruptive incidents to the organization?*
- 13.4 Are specific response and recovery strategies defined for the prioritized activities?*
- 13.5 Are formal business continuity procedures developed and documented?*
- 13.6 Has senior management assigned the responsibility for the overall management of the response and recovery efforts?*
- 13.7 Is there a periodic (at least annual) review of your Business Resiliency Program?*
- 13.8 Are there any dependencies on critical third party service providers?*
- 13.9 Is there a formal, documented exercise and testing program in place?*
- 13.10 Is there an Influenza Pandemic / Infectious Disease Outbreak Plan?*
- 13.11 Is there a specific Recovery Time Objective (RTO)? If yes, what is it?*
- 13.12 Are all suppliers of critical hardware, network services and facility services involved in annual continuity and recovery tests?*
- 13.13 Are site failover tests performed at least annually?*
- 13.14 Do contracts with Critical Service Providers include a penalty or remediation clause for breach of availability and continuity SLAs?*

13.15 Is there sufficient redundancy capacity to ensure services are not impacted in multi-tenancy environments during peak usage and above?*

14. Compliance

- 14.1 Is there an internal audit, risk management, or compliance department, or similar management oversight unit with responsibility for assessing, identifying and tracking resolution of outstanding regulatory issues?***
- 14.2 Are there policies and procedures to ensure compliance with applicable legislative, regulatory and contractual requirements including intellectual property rights on business processes or information technology software products?***
- 14.3 Is there a records retention policy covering paper and electronic records, including email in support of applicable regulations, standards and contractual requirements?***
- 14.4 Is licensing maintained in all jurisdictions where required?***
- 14.5 Is there an documented internal compliance and ethics program to ensure professional ethics and business practices are implemented and maintained?***
- 14.6 Are marketing or selling activities conducted directly to Client's customers?***
- 14.7 Are there direct interactions with your client's customers?***
- 14.8 Are documented policies and procedures maintained for enabling compliance with applicable legal, regulatory, or contractual obligations related to information security requirements?***
- 14.9 Is there a documented governance process to identify and assess changes that could significantly affect the system of internal controls for security, confidentiality and availability?***
- 14.10 Are accounts opened, transactions initiated or other account initiation activity applying payments, taking payments, transferring funds, etc. through either electronic, telephonic, written or in-person requests made on behalf of your client's?***
- 14.11 Are these sites, applications and systems used to also transmit, process or store non-scoped data?***
- 14.12 Are all transaction details (such as payment card info and information about the parties conducting transactions) prohibited from being stored in the DMZ?***

14.13 Does the service provider permit client audits and assessments?*

15. End User Device Security

15.1 Are End User Devices (Desktops, Laptops, Tablets, Smartphones) used for transmitting, processing or storing Scoped Data? If yes, for all platforms, are:*

15.1.1 Security configuration standards documented?*

15.1.2 All available high-risk security patches applied and verified at least monthly on all server platforms?*

15.1.3 Sufficient detail contained in Operating System and application logs to support incident investigation, including successful and failed login attempts and changes to sensitive configuration settings and files?*

15.1.4 Operating system and application logs relevant to supporting incident investigation protected against modification, deletion, and/or inappropriate access?*

15.2 Are constituents allowed to utilize mobile devices within your environment? If yes, which of the following functions are allowed:*

15.2.1 View Scoped Data?*

15.2.2 Process Scoped Data?*

15.2.3 Delete Scoped Data?*

15.2.4 Store Scoped Data?*

15.3 Is there a mobile device management program in place that has been approved by management and communicated to appropriate constituents?*

15.4 Is there a Mobile Device Management solution in place?*

15.5 Is there an approved process for IT to off-board mobile devices when a constituent terminates, or requests to on-board a new mobile device?*

15.6 Are staff technically prevented from accessing the administrative environment via non-managed private devices?*

16. Network Security

16.1 Are there external network connections (Internet, extranet, etc.)?*

16.2 Security and hardening standards for network devices, including Firewalls, Switches, Routers and Wireless Access Points (baseline configuration, patching, passwords, access control)?*

16.3 Are firewalls used to isolate critical and sensitive systems into network segments separate from network segments with less sensitive systems?*

16.4 Is there a process that requires security approval to allow external networks to connect to the company network, and enforces the least privilege necessary?*

16.5 Are all available high-risk security patches applied and verified at least monthly?*

16.6 Are Intrusion Detection/Prevention Systems employed in all sensitive network zones and wherever firewalls are enabled?*

16.7 Are wireless networking devices connected to networks containing scoped systems and data?*

16.8 Are there controls to prevent one client attempting to compromise another client in a resource pooled environment?*

17. Privacy

- 17.1** Is Scoped Data transmitted, processed, or stored that can be classified as non-public information (NPI), personally identifiable information (PII), or sensitive customer financial information? If yes, describe and list types of data.*
- 17.2** Do agreements with third parties who have access or potential access to Scoped Data, address confidentiality, audit, security, and privacy, including but not limited to incident response, ongoing monitoring, data sharing and secure disposal of Scoped Data?*
- 17.3** Is a business associate contract in place to address obligations for the privacy and security requirements for the services provided?*
- 17.4** For Scoped Data, is personal information about individuals transmitted to or received from countries outside the United States? If yes, list the countries.*
- 17.5** Is personal information transmitted, processed, stored, or disclosed to or retained by third parties? If yes, describe.*
- 17.5.1** Are there contractual controls to ensure that personal information transmitted, processed, stored or disclosed to or retained by third parties is limited to defined parameters for access, use and disclosure? If yes, describe. If no, explain reason.*
- 17.5.2** Is personal information accessed, disclosed, processed, transmitted or retained with third parties outside the US? If yes, describe and list the countries.*
- 17.5.3** Is there a documented privacy policy or procedures for the protection of information transmitted, processed, or maintained on behalf of the client?*
- 17.6** Are transactions for covered accounts accessed, modified, or processed, including address changes and discrepancies? If yes, describe.*

18. Threat Management

18.1 Is there an anti-malware policy or program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?*

18.1.1 Prohibition of disabling anti-malware with exceptions requiring Security approval and reenabling as soon as possible.*

18.2 Is there a vulnerability management policy or program that has been approved by management, communicated to appropriate constituents and an owner assigned to maintain and review the policy?*

18.3 Are vulnerability scans performed on all internet-facing applications at least monthly and after significant changes?*

18.4 Are vulnerability scans performed against internal networks and systems?*

18.5 Are penetration tests performed?*

18.6 Are there processes to manage threat and vulnerability assessment tools and the data they collect?*

19. Server Security

19.1 Are Servers used for transmitting, processing or storing Scoped Data?*

19.2 Are systems and applications patched?*

19.3 Are default hardened base virtual images applied to virtualized operating systems?*

19.4 Are Hypervisors used to manage systems used to transmit, process or store Scoped Data?*