SIG Lite
Security Assessment Questionnaire

Standardized Information Gathering v2017.1 · Free resource from RSystems NYC

Governance / Risk | Assets / Devices | Human Resources | Physical | Operations | Access Control | Applications | Incidents / Threats | Compliance | Network / Privacy

ORGANIZATION NAME

PRIMARY CONTACT

TITLE / ROLE

EMAIL ADDRESS

PHONE NUMBER

ASSESSMENT DATE

SERVICE / RELATIONSHIP SCOPE

VENDOR / PROVIDER NAME

How to Complete This Questionnaire

- For each question, select Yes, No, IDK (I Don't Know), or N/A.
- Use Additional Notes to explain — especially for No, IDK, or N/A answers.
- Honest responses are more useful and safer than inflated ones.
- Misrepresenting controls creates liability if a breach occurs.
- "Scoped Data" = systems and data relevant to this specific service relationship.
- A SOC 2 Type II report, if available, is generally preferred over a completed SIG Lite.
- For help completing or interpreting this form: rsystems.nyc

A. Risk Assessment and Treatment

	QUESTION / REQUIREMENT	YES	NO	IDK	N/A	ADDITIONAL NOTES
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:	☐	☐	☐	☐	
2	Is there a program to manage the treatment of risks identified during assessments?	☐	☐	☐	☐	
3	A formal process for assigning appropriate management ownership for each risk?	☐	☐	☐	☐	
4	A formal process for appropriate management knowingly and objectively accepting risks and approving action plans?	☐	☐	☐	☐	
5	A formal process for tracking the status of action plans and reporting them to management?	☐	☐	☐	☐	
6	Controls identified for each material risk?	☐	☐	☐	☐	
7	Measures for defining, monitoring, and reporting risk metrics?	☐	☐	☐	☐	
8	Do Subcontractors have access to Scoped Systems and Data? (backup vendors, service providers, equipment support maintenance, software maintenance vendors, data recovery vendors, etc.)? If yes, is there:	☐	☐	☐	☐	
9	A documented vendor management process in place for the selection, oversight and risk assessment of third party vendors? If yes, does it include:	☐	☐	☐	☐	
10	Approval by management?	☐	☐	☐	☐	
11	Annual review?	☐	☐	☐	☐	
12	Required reassessment when service delivery or contract changes?	☐	☐	☐	☐	
13	Review of the subcontractor's vendor management policy and procedures?	☐	☐	☐	☐	
14	Is there a process to identify and log subcontractor information security, privacy and/or data breach issues?	☐	☐	☐	☐	
15	Is there a vendor management program?	☐	☐	☐	☐	
16	Do external parties have access to Scoped Systems and Data or processing facilities?	☐	☐	☐	☐	

A. Risk Assessment and Treatment (continued)

	QUESTION / REQUIREMENT	YES	NO	IDK	N/A	ADDITIONAL NOTES
17	Is the maturity of IT management processes formally evaluated at least annually using an established benchmark (e.g., COBIT maturity models)?	☐	☐	☐	☐	
18	Are there regular privacy risk assessments conducted? If yes, provide frequency and scope. If no, explain reason.	☐	☐	☐	☐	
19	Are identified privacy risks and associated mitigation plans formally documented and reviewed by management?	☐	☐	☐	☐	
20	Are reasonable resources (in time and money) allocated to mitigating identified privacy risks?	☐	☐	☐	☐	
21	Is there a compliance risk management system that addresses the quality and accuracy of reported consumer data?	☐	☐	☐	☐	
22	Is there a compliance risk management system that addresses the quality of assembling and maintaining the data?	☐	☐	☐	☐	

B. Security Policy

	QUESTION / REQUIREMENT	YES	NO	IDK	N/A	ADDITIONAL NOTES
23	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?	☐	☐	☐	☐	
24	Have the policies been reviewed in the last 12 months?	☐	☐	☐	☐	

C. Organizational Security

	QUESTION / REQUIREMENT	YES	NO	IDK	N/A	ADDITIONAL NOTES
25	Is there a respondent information security function responsible for security initiatives?	☐	☐	☐	☐	

D. Asset and Information Management

	QUESTION / REQUIREMENT	YES	NO	IDK	N/A	ADDITIONAL NOTES
26	Is there an asset management policy approved by management, communicated to constituents and an owner to maintain and review?	☐	☐	☐	☐	
27	Is information classified?	☐	☐	☐	☐	

D. Asset and Information Management (continued)

	QUESTION / REQUIREMENT	YES	NO	IDK	N/A	ADDITIONAL NOTES
28	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?	☐	☐	☐	☐	
29	Is Scoped Data sent or received via physical media?	☐	☐	☐	☐	
30	Are encryption tools managed and maintained for Scoped Data? If yes:	☐	☐	☐	☐	
31	Are clients provided with the ability to generate a unique encryption key?	☐	☐	☐	☐	
32	Are clients provided with the ability to rotate their encryption key on a scheduled basis?	☐	☐	☐	☐	
33	Are staff able to access client Scoped Data in an unencrypted state?	☐	☐	☐	☐	
34	Are staff able to access client's encryption keys?	☐	☐	☐	☐	
35	Is data segmentation and separation capability between clients provided?	☐	☐	☐	☐	
36	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?	☐	☐	☐	☐	
37	Is there a data classification retention program that identifies the data types that require additional management and governance?	☐	☐	☐	☐	
38	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?	☐	☐	☐	☐	

E. Human Resource Security

	QUESTION / REQUIREMENT	YES	NO	IDK	N/A	ADDITIONAL NOTES
39	Is there a Human Resource policy approved by management, communicated to constituents and an owner to maintain and review? If yes, does it include:	☐	☐	☐	☐	
40	Security roles and responsibilities?	☐	☐	☐	☐	
41	Background screening?	☐	☐	☐	☐	

E. Human Resource Security (continued)

	QUESTION / REQUIREMENT	YES	NO	IDK	N/A	ADDITIONAL NOTES
42	Employment agreements?	☐	☐	☐	☐	
43	Security awareness training?	☐	☐	☐	☐	
44	Disciplinary process for non-compliance?	☐	☐	☐	☐	
45	Termination or change of status process?	☐	☐	☐	☐	
46	Are background checks performed for Service Provider Contractors and Subcontractors?	☐	☐	☐	☐	
47	Do information security personnel have professional security certifications?	☐	☐	☐	☐	

F. Physical and Environmental Security

	QUESTION / REQUIREMENT	YES	NO	IDK	N/A	ADDITIONAL NOTES
48	Is there a physical security program?	☐	☐	☐	☐	
49	Are physical security and environmental controls in the data center and office buildings?	☐	☐	☐	☐	
50	Are visitors permitted in the facility?	☐	☐	☐	☐	

G. Operations Management

	QUESTION / REQUIREMENT	YES	NO	IDK	N/A	ADDITIONAL NOTES
51	Are management approved operating procedures utilized?	☐	☐	☐	☐	
52	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?	☐	☐	☐	☐	
53	Are backups of Scoped Systems and Data performed?	☐	☐	☐	☐	
54	Are Cloud Services provided? If yes, what service model is provided (select all that apply):	☐	☐	☐	☐	
55	Software as a Service (SaaS)?	☐	☐	☐	☐	
56	Infrastructure as a Service (IaaS)?	☐	☐	☐	☐	
57	Private cloud?	☐	☐	☐	☐	
58	Public cloud?	☐	☐	☐	☐	

G. Operations Management (continued)

	QUESTION / REQUIREMENT	YES	NO	IDK	N/A	ADDITIONAL NOTES
59	Community cloud?	☐	☐	☐	☐	
60	Hybrid cloud?	☐	☐	☐	☐	
61	Is there a client management portal which allows distributed business accounts (business units/departments) to be managed under a single central corporate account?	☐	☐	☐	☐	
62	Are application self service features or an Internet accessible self-service portal available to clients?	☐	☐	☐	☐	
63	Can clients run their own security services within their own cloud environment?	☐	☐	☐	☐	
64	Is there a management approved process to ensure that image snapshots containing Scoped Data are authorized prior to being snapped?	☐	☐	☐	☐	
65	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:	☐	☐	☐	☐	
66	Is there a scheduled maintenance window? If yes, what is the frequency:	☐	☐	☐	☐	
67	Is there a scheduled maintenance window which results in client downtime? If yes, what is the downtime:	☐	☐	☐	☐	
68	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:	☐	☐	☐	☐	

H. Access Control

	QUESTION / REQUIREMENT	YES	NO	IDK	N/A	ADDITIONAL NOTES
69	Are electronic systems used to transmit, process or store Scoped Systems and Data?	☐	☐	☐	☐	
70	Are individual IDs required for user authentication to applications, operating systems, databases and network devices?	☐	☐	☐	☐	
71	Are passwords used?	☐	☐	☐	☐	
72	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?	☐	☐	☐	☐	

H. Access Control (continued)

	QUESTION / REQUIREMENT	YES	NO	IDK	N/A	ADDITIONAL NOTES
73	Is remote access permitted?	☐	☐	☐	☐	
74	Is standards based federated ID capability available to clients (e.g., SAML, OpenID)?	☐	☐	☐	☐	
75	Is two factor authentication required to access the production environment containing Scoped Data?	☐	☐	☐	☐	
76	Are staff able to access client Scoped Data? If not, please identify the controls used to prevent this.	☐	☐	☐	☐	
77	Is there a process which allows the client to specifically list who from the provider will have access to their Scoped Systems and Data?	☐	☐	☐	☐	

I. Application Security

	QUESTION / REQUIREMENT	YES	NO	IDK	N/A	ADDITIONAL NOTES
78	Are applications used to transmit, process or store Scoped Data?	☐	☐	☐	☐	
79	Is a web site supported, hosted or maintained that has access to Scoped Systems and Data?	☐	☐	☐	☐	
80	Are Web Servers used for transmitting, processing or storing Scoped Data? If yes, for all server platforms is/are:	☐	☐	☐	☐	
81	Is HTTPS enabled for all web pages used as part of the scoped service?	☐	☐	☐	☐	
82	All available high-risk security patches applied and verified at least monthly?	☐	☐	☐	☐	
83	Are third party alert services used to keep up to date with the latest vulnerabilities?	☐	☐	☐	☐	
84	Events relevant to supporting incident investigation regularly reviewed using a specific methodology to uncover potential incidents?	☐	☐	☐	☐	
85	Operating system and application logs relevant to supporting incident investigation protected against modification, deletion, and/or inappropriate access?	☐	☐	☐	☐	
86	Is application development performed?	☐	☐	☐	☐	

I. Application Security (continued)

	QUESTION / REQUIREMENT	YES	NO	IDK	N/A	ADDITIONAL NOTES
87	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?	☐	☐	☐	☐	
88	Is development, test, and staging environment separate from the production environment? If so, how are they segmented:	☐	☐	☐	☐	
89	Is there a formal Software Development Life Cycle (SDLC) process?	☐	☐	☐	☐	
90	Are change control procedures required for all changes to the production environment?	☐	☐	☐	☐	
91	Is Scoped Systems and Data ever used in the test, development, or QA environments? If yes, is:	☐	☐	☐	☐	
92	Is there a documented change management / change control process? If yes, does it include:	☐	☐	☐	☐	
93	Are compilers, editors or other development tools present in the production environment?	☐	☐	☐	☐	
94	Is a secure code review performed at least annually?	☐	☐	☐	☐	
95	Is each release subject to a full secure code review?	☐	☐	☐	☐	
96	Are applications analyzed on a regular basis to determine their vulnerability against recent attacks?	☐	☐	☐	☐	
97	Is there a formal development methodology in operation? If yes, which groups does it include?:	☐	☐	☐	☐	
98	Are mobile applications that access Scoped Systems and Data developed?	☐	☐	☐	☐	

J. Incident Event and Communications Management

	QUESTION / REQUIREMENT	YES	NO	IDK	N/A	ADDITIONAL NOTES
99	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:	☐	☐	☐	☐	
100	Privacy Incidents?	☐	☐	☐	☐	

J. Incident Event and Communications Management (continued)

	QUESTION / REQUIREMENT	YES	NO	IDK	N/A	ADDITIONAL NOTES
101	Is there a formal Incident Response Plan?	☐	☐	☐	☐	
102	Is there a 24x7x365 staffed phone number available to clients to report security incidents?	☐	☐	☐	☐	

K. Business Resiliency

	QUESTION / REQUIREMENT	YES	NO	IDK	N/A	ADDITIONAL NOTES
103	Is there an established Business Resiliency program that has been approved by management and communicated to appropriate constituents?	☐	☐	☐	☐	
104	Has a Business Impact Analysis been conducted?	☐	☐	☐	☐	
105	Is there a formal process focused on identifying and addressing risks of disruptive incidents to the organization?	☐	☐	☐	☐	
106	Are specific response and recovery strategies defined for the prioritized activities?	☐	☐	☐	☐	
107	Are formal business continuity procedures developed and documented?	☐	☐	☐	☐	
108	Has senior management assigned the responsibility for the overall management of the response and recovery efforts?	☐	☐	☐	☐	
109	Is there a periodic (at least annual) review of your Business Resiliency Program?	☐	☐	☐	☐	
110	Are there any dependencies on critical third party service providers?	☐	☐	☐	☐	
111	Is there a formal, documented exercise and testing program in place?	☐	☐	☐	☐	
112	Is there an Influenza Pandemic / Infectious Disease Outbreak Plan?	☐	☐	☐	☐	
113	Is there a specific Recovery Time Objective (RTO)? If yes, what is it?	☐	☐	☐	☐	
114	Are all suppliers of critical hardware, network services and facility services involved in annual continuity and recovery tests?	☐	☐	☐	☐	
115	Are site failover tests performed at least annually?	☐	☐	☐	☐	
116	Do contracts with Critical Service Providers include a penalty or remediation clause for breach of availability and continuity SLAs?	☐	☐	☐	☐	

K. Business Resiliency (continued)

	QUESTION / REQUIREMENT	YES	NO	IDK	N/A	ADDITIONAL NOTES
117	Is there sufficient redundancy capacity to ensure services are not impacted in multi-tenancy environments during peak usage and above?	☐	☐	☐	☐	

L. Compliance

	QUESTION / REQUIREMENT	YES	NO	IDK	N/A	ADDITIONAL NOTES
118	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?	☐	☐	☐	☐	
119	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?	☐	☐	☐	☐	
120	Is there a records retention policy covering paper and electronic records, including email in support of applicable regulations, standards and contractual requirements?	☐	☐	☐	☐	
121	Is licensing maintained in all jurisdictions where required?	☐	☐	☐	☐	
122	Is there an documented internal compliance and ethics program to ensure professional ethics and business practices are implemented and maintained?	☐	☐	☐	☐	
123	Are marketing or selling activities conducted directly to Client's customers?	☐	☐	☐	☐	
124	Are there direct interactions with your client's customers?	☐	☐	☐	☐	
125	Are documented policies and procedures maintained for enabling compliance with applicable legal, regulatory, or contractual obligations related to information security requirements?	☐	☐	☐	☐	
126	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?	☐	☐	☐	☐	

L. Compliance (continued)

	QUESTION / REQUIREMENT	YES	NO	IDK	N/A	ADDITIONAL NOTES
127	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?	☐	☐	☐	☐	
128	Are these sites, applications and systems used to also transmit, process or store non-scoped data?	☐	☐	☐	☐	
129	Are all transaction details (such as payment card info and information about the parties conducting transactions) prohibited from being stored in the DMZ?	☐	☐	☐	☐	
130	Does the service provider permit client audits and assessments?	☐	☐	☐	☐	

M. End User Device Security

	QUESTION / REQUIREMENT	YES	NO	IDK	N/A	ADDITIONAL NOTES
131	Are End User Devices (Desktops, Laptops, Tablets, Smartphones) used for transmitting, processing or storing Scoped Data? If yes, for all platforms, are:	☐	☐	☐	☐	
132	Security configuration standards documented? If yes, are:	☐	☐	☐	☐	
133	All available high-risk security patches applied and verified at least monthly on all server platforms?	☐	☐	☐	☐	
134	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?	☐	☐	☐	☐	
135	Operating system and application logs relevant to supporting incident investigation protected against modification, deletion, and/or inappropriate access?	☐	☐	☐	☐	
136	Are constituents allowed to utilize mobile devices within your environment? If yes, which of the following functions are allowed:	☐	☐	☐	☐	
137	View Scoped Data?	☐	☐	☐	☐	
138	Process Scoped Data?	☐	☐	☐	☐	
139	Delete Scoped Data?	☐	☐	☐	☐	

M. End User Device Security (continued)

	QUESTION / REQUIREMENT	YES	NO	IDK	N/A	ADDITIONAL NOTES
140	Store Scoped Data?	☐	☐	☐	☐	
141	Is there a mobile device management program in place that has been approved by management and communicated to appropriate constituents?	☐	☐	☐	☐	
142	Is there a Mobile Device Management solution in place?	☐	☐	☐	☐	
143	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? If yes, does it:	☐	☐	☐	☐	
144	Are staff technically prevented from accessing the administrative environment via non-managed private devices? If yes, is it from:	☐	☐	☐	☐	

N. Network Security

	QUESTION / REQUIREMENT	YES	NO	IDK	N/A	ADDITIONAL NOTES
145	Are there external network connections (Internet, extranet, etc.)?	☐	☐	☐	☐	
146	Security and hardening standards for network devices, including Firewalls, Switches, Routers and Wireless Access Points (baseline configuration, patching, passwords, access control)?	☐	☐	☐	☐	
147	Are firewalls used to isolate critical and sensitive systems into network segments separate from network segments with less sensitive systems?	☐	☐	☐	☐	
148	Is there a process that requires security approval to allow external networks to connect to the company network, and enforces the least privilege necessary?	☐	☐	☐	☐	
149	Are all available high-risk security patches applied and verified at least monthly?	☐	☐	☐	☐	
150	Are Intrusion Detection/Prevention Systems employed in all sensitive network zones and wherever firewalls are enabled?	☐	☐	☐	☐	
151	Are wireless networking devices connected to networks containing scoped systems and data?	☐	☐	☐	☐	
152	Are there controls to prevent one client attempting to compromise another client in a resource pooled environment?	☐	☐	☐	☐	

P. Privacy

	QUESTION / REQUIREMENT	YES	NO	IDK	N/A	ADDITIONAL NOTES
153	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.	☐	☐	☐	☐	
154	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?	☐	☐	☐	☐	
155	Is a business associate contract in place to address obligations for the privacy and security requirements for the services provided?	☐	☐	☐	☐	
156	For Scoped Data, is personal information about individuals transmitted to or received from countries outside the United States? If yes, list the countries.	☐	☐	☐	☐	
157	Is personal information transmitted, processed, stored, or disclosed to or retained by third parties? If yes, describe.	☐	☐	☐	☐	
158	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.	☐	☐	☐	☐	
159	Is personal information accessed, disclosed, processed, transmitted or retained with third parties outside the US? If yes, describe and list the countries.	☐	☐	☐	☐	
160	Is there a documented privacy policy or procedures for the protection of information transmitted, processed, or maintained on behalf of the client?	☐	☐	☐	☐	
161	Are transactions for covered accounts accessed, modified, or processed, including address changes and discrepancies? If yes, describe.	☐	☐	☐	☐	

T. Threat Management

	QUESTION / REQUIREMENT	YES	NO	IDK	N/A	ADDITIONAL NOTES
162	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?	☐	☐	☐	☐	

T. Threat Management (continued)

	QUESTION / REQUIREMENT	YES	NO	IDK	N/A	ADDITIONAL NOTES
163	Prohibition of disabling anti-malware with exceptions requiring Security approval and reenablement as soon as possible.	☐	☐	☐	☐	
164	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?	☐	☐	☐	☐	
165	Are vulnerability scans performed on all internet-facing applications at least monthly and after significant changes?	☐	☐	☐	☐	
166	Are vulnerability scans performed against internal networks and systems?	☐	☐	☐	☐	
167	Are penetration tests performed?	☐	☐	☐	☐	
168	Are there processes to manage threat and vulnerability assessment tools and the data they collect?	☐	☐	☐	☐	

U. Server Security

	QUESTION / REQUIREMENT	YES	NO	IDK	N/A	ADDITIONAL NOTES
169	Are Servers used for transmitting, processing or storing Scoped Data?	☐	☐	☐	☐	
170	Are systems and applications patched?	☐	☐	☐	☐	
171	Are default hardened base virtual images applied to virtualized operating systems?	☐	☐	☐	☐	
172	Are Hypervisors used to manage systems used to transmit, process or store Scoped Data?	☐	☐	☐	☐	