SHARED ASSESSMENTS

SHARED ASSESSMENTS PROGRAM SIG 2014 OVERVIEW

THE SIG

The Standard Information Gathering ("SIG") questionnaire is a compilation of questions to determine how information technology and data security risks are managed across a broad spectrum of risk control areas. As such, it addresses risk controls across 15 different risk areas. The robust set of questions contained in the SIG are reviewed annually for updates and revisions, and are based on referenced industry standards (FFIEC, ISO, COBIT and PCI). New risk areas are added on a regular basis, with Cloud services and mobile device security as examples of some of the more recent additions.

The SIG provides its users with a standardized tool to gather pertinent information about the technology, operating and data security controls, within a third-party's environment. The SIG was developed to enable a service provider to compile complete information about these risk areas in one document. By compiling all of this information in one document, a service provider is able to complete one questionnaire, which can then be shared with multiple clients. This avoids the time consuming and expensive requirement of completing multiple questionnaires for multiple clients. It can be used in a number of ways, by both the contracting company (issuer) and the third party they have engaged to provide services (responder).

Listed below are ways the SIG can be utilized:

- **Used by a company outsourcing services** (issuer) to evaluate their vendors' technology and data security risk controls.
- **Completed by a service provider** and used proactively as part of a Request For Proposal (RFP) response.
- **Completed by a service provider** and sent to their client(s) in lieu of completing multiple proprietary questionnaires.
- **A self-assessment of risks and responses.** If a service provider provides you with a SIG, ensure its scope meets your needs in terms of business service provided, breadth of risks to that service and range of responses to those risks (realizing that responses include more than controls).

HOW TO USE THE SIG

This section describes the use of the SIG and how to use/scope each of the tabs.

Please note: *This Guide is not intended to offer specific recommendations for vendor assessment and/or risk management practices. Its purpose is to provide guidance on the use of the SIG.*

Creating a Master SIG

It is useful for a company that issues the SIG to its vendors to create a master SIG by vendor service type. The creation of a master SIG allows the issuer to compare the SIG it receives from its vendors to the set of risk controls it believes should be in place. This facilitates the identification of risk control areas, which require additional examination, and/or areas that require remediation.

SHARED ASSESSMENTS

SIG Management Tool (SMT)

The SMT is a companion tool to the SIG and performs two primary functions:

1. Automates the ability to compare a master SIG to SIGs received from vendors by producing a detailed report, which identifies discrepancy between the desired responses in the master SIG and the responses provided by the vendor.
2. SMT allows a user to transfer responses between SIG versions. This allows a user to transfer responses to a newer version of the SIG and only complete sections not previously addressed. It also facilitates the transfer to older versions of the SIG, should it be required.

Scoping

Scope definition is the most important step in completing a SIG. To make effective use of the SIG, it is essential that time be devoted to determining what areas of the SIG apply to the specific set of services being provided by the vendor to whom the SIG will be sent for completion. Because the SIG represents a broad range of potential controls applicable to a number of technology and security risk standards, it includes a substantial list of assets, processes and controls. When developing your SIG, focus on the risk controls relevant to the services provided. For example, you may have different risk control requirements for an onsite-shredding provider than for a contract data processor. Therefore it is essential to take the time to establish the scope of the SIG for each vendor type, and to communicate that scope to the vendor when providing the SIG for completion.

The need to fully refine the scope of the SIG arises from the way in which a service is provided (e.g., location, infrastructure, platforms or processing environments) in accordance with the service agreement.

TAB DESCRIPTION, USE, AND GUIDANCE

This section describes the use and guidance for each of the tabs, along with information common to all the tabs in the SIG.

SIG Automation

There are two levels of automation built into the SIG. The highest level of automation includes the use of macros to dynamically generate questions and facilitate certain tasks. However, if an organization restricts the use of macros, a more basic level of functionality remains, which relies on formulas and conditional formatting.

Please note: *There are differences in the look and feel of the SIG based on whether macros are enabled. Thus, it is important to initially determine whether you are going to use the SIG with or without macros enabled.*

Macros Enabled

- Top-level questions will initially be displayed in the tab.
- Sub-questions on the tabs will either be displayed or suppressed depending on the response to the top-level question. For example, if yes is selected the sub-level questions will be displayed. If no or N/A is selected, the sub-level question(s) will remain suppressed. .

SHARED ASSESSMENTS

Please note: *To disable macros for a specific tab(s) check the* Disable Tab Automation *checkbox at the top of the tab. When checked, all questions will be displayed.*

Macros Disabled

All questions on the detail tab will be displayed if macros are disabled.

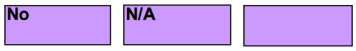
SIG Color Key

Password protection is used to restrict changes to the SIG. Therefore, colors are used to identify cells that can be changed. It is important to note that neither the content, nor the color codes indicate an endorsement of the "correctness" of the response. The issuer, in terms of their own needs, decides the relevance and importance of each response.

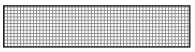
The following are the colors used in the SIG and a description for each:

LIGHT BLUE BACKGROUND IN A CELL indicates cells that are not protected and allow text to be entered or edited. Cells with this color are located on the Dashboard, Business Information, Documentation, and all detail tabs.

GREEN BACKGROUND IN A CELL identifies a "Yes" response to a question, whether or not the word "Yes" appears. If the text "Yes" does not appear in a green cell, then the response was inherited by the answer to the top-level question (see Question Hierarchy below for more detail).



PURPLE BACKGROUND IN A CELL identifies a "No" or "N/A" response to a question, whether or not the word "No" appears. If the text "No" or "N/A" does not appear in a purple cell, then the response was inherited by the answer to its top-level question (see Question Hierarchy below for more detail).



CELLS WITH A HASH BACKGROUND are not to be filled in; rather they are a primary question with secondary questions below.

A YELLOW BACKGROUND ON THE TOP OF A TAB indicates the tab is incomplete. In addition to being found in an incomplete tab, the yellow background will appear on the Dashboard, Lite, and Business Information tabs to indicate where responses are still required. (See below for more information on the purpose of the Dashboard.)

A GREEN BACKGROUND ON THE TOP OF A TAB indicates the tab is complete. In addition to being found in a complete tab, the green background will appear on the Dashboard, Lite, and Business Information tabs to indicate where responses are still required. (See below for more information on the purpose of the Dashboard.)

Question Hierarchy

SIG questions are arranged hierarchically, top-level question followed by sub-questions, when appropriate. This hierarchy is identified by the question number, and the number of digits and separators (a period), which identify the relationship of the question (e.g., question A.1.1 is a sub-level of A.1). If a "No" or "N/A" response is provided for question A.1, question

A.1.1 will inherit that response. This inherence is indicated by the background color of the response cell (see SIG Color Key above). Signage on each table in the luncheon area with your organization's logo and name.

SIG Errors and Recovery

Since the SIG uses formulas and macros for calculations, altering the SIG may generate worksheet errors. While content may be altered; users are advised against the deletion and/or addition of columns or rows. The preferable manner to perform these alterations is to "hide" columns or rows.

SIG TABS

Instructions

The Instruction section gives basic instructions for using the SIG. This field is editable so customized instructions can be provided, if necessary.

Respondent Instructions	Issuer Instructions
Review the request provided by your client/customer which should provide you with instructions on how to answer the SIG and detail the sections of the SIG you are required to complete. If you did not receive instructions from your client we recommend you contact them and seek guidance on how they need the SIG answered and the sections they require you to complete. As you complete the SIG certain cells may change color or if Excel macros are enabled the questions may not be displayed. Based on your response, the SIG will either display questions and/or the response field will change color. This will reduce the number of questions you are required to answer. Primary or parent questions are followed by numbered sub-questions. If you answer 'No' or 'N/A' to a question that cell and all of its related sub-questions will either be hidden and/or the response field will turn purple indicating that you do NOT have to provide a response for those questions. They will show as 'No' or 'N/A' to the Issuer of the SIG when they receive your response. There are two parts to this questionnaire: - SIG Lite - Detail tabs (A through V). The instructions below will help you in the completion of the SIG Lite or full SIG.	We recommend that prior to issuing the SIG you rev vendor should answer based on the type of service(We recommend that along with the SIG, you provide they are required to answered and any other informa accurately complete the SIG (additional questions, c Detailed instructions on how to use the SIG are cont which also includes a Respondent Guide you may w **SIG Management Tool (SMT)** A macros-enabled spreadsheet is provided to Issuer service provider responses and managing the transf previous versions of the SIG. If a master SIG is crea comparisons of all responses in the master SIG to th provider. The SMT will also transfer responses and t field from previous versions of the SIG. For a full list to the SMT Functionality tab. **Note:** Detailed instructions for the use of the SMT a

Use and modify the instructions tab to suit your needs

Dashboard

The Dashboard allows the user to quickly see which tabs of the SIG are completed. The values show the percentage of question completion for each tab. All of the tab names in the Dashboard section are hyperlinks, when you click on the link you are taken to that tab.

SHARED ASSESSMENTS

Dashboard	Tabs
The Dashboard provides you with a quick and easy reference to determine if the required sections of the SIG have been completed. As questions are answered, either directly or by being pre-filled, the Dashboard will track the completion percentage of each section.	Terms Of Use Business Information Documentation Request List SIG Lite A. Risk Management B. Security Policy C. Organizational Security D. Asset Management E. Human Resources Security F. Physical and Environmental G. Communications and Operations Ma H. Access Control I. Information Systems Application Deve J. Incident Event and Communications M K. Business Continuity and Disaster Rec L. Compliance M. Mobile P. Privacy

Track your progress using the dynamically updated SIG dashboard

Business Information

The Business Information tab is where the Responder provides information about the organization and defines the scope of the SIG. If the SIG is used as a self-assessment tool, only the last sections (Scope) should be completed.

Business Information	
19 Total Questions to be Answered	**0% Percent Complete**
Question/Request	**Response**
Responder Name	
Responder Job Title	
Responder Contact Information	
Names and titles/functions of individuals who contributed to this questionnaire	
Date of Response	
Company Profile	
Name of the holding or parent company	
Company/business name	
Publicly or privately held company	
If public, what is the name of the Exchange	
If public, what is the trading symbol	
Type of legal entity and state of incorporation	
How long has the company been in business	
Are there any material claims or judgments against the company	
If yes, describe the impact it may have on the services in scope of this document	

Responder business information

Documentation

The Documentation tab provides a list of suggested documents to include with the SIG and a way for the Responder to identify which documents were provided.

SHARED ASSESSMENTS

Documentation*
Use this section to request any specific documentation you want the Respondent to provide along with the SIG

Document Request	Question Reference	Name and/or type of information provided (e.g document, summary, table of contents)
* 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		
* Copy of internal or external information security audit report		
Information technology and security organization charts (including where information security resides in the organization and the composition of any information security		

Keep track of essential, associated documentation

Lite

This tab can be used as a standalone questionnaire in lieu of the entire SIG. The Lite tab consists of a subset of questions duplicated from all of the detail tabs for the full SIG. It is generally used for vendors who offer lower risk services, but can also be used as a starting point to conduct an initial assessment of all vendors. Responses provided on the Lite tab are transferred to their corresponding questions on each detail tab. This avoids the need to copy answers from the Lite tab to a detailed tab if it is required that a full SIG is required.

SIG Lite

121 Total Questions to be Answered — 0% Percent Complete

Questionnaire Instructions:
- For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory, use the Additional Information field to the

Ques Num	Question/Request	Response	Additional Information	AUP Reference
	A. Risk Assessment and Treatment			
SL.1	Is there a risk assessment program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the program?			A.1 IT & Infrastructure Risk Governance and Context
	B. Security Policy			
SL.2	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?			
SL.3				
	C. Organizational Security			
SL.4	Is there an information security function responsible for security initiatives within the organization?			
SL.5				
	D. Asset Management			
SL.6	Is there an asset management policy or program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?			

Speed your initial evaluation process by using the included SIG Lite

SHARED ASSESSMENTS

Glossary

The Glossary contains a list of terms used within the SIG. All terms included in the Glossary are italicized in the SIG.

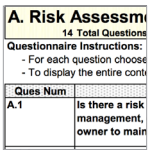
Glossary	
Term	**Definition**
Acceptable Use Policy	Part of the information security framework that defines what users are and are not a organization. It should contain a subset of the information security policy and refer relevant. It should also clearly define the sanctions applied if a user violates the pol
Acknowledgement of Acceptable Use	A written attestation from a user of an information system indicating the user's acce the relevant information systems control policies.
Anti-Tailgating / Anti-Piggybacking Mechanism	Two sets of doors whereby access to the second is not granted until the individual first, often referred to as a "man trap." A controlled turnstile is also considered an a
Asset Classification	The category or type assigned to an asset, which is derived from the asset classific frequently vary from company to company.
Asset Control Tag	A unique identification number assigned to all inventoried assets.
Attribute	A property or field of a particular object.
Baseline	A benchmark by which subsequent items are measured.
Battery	An electrochemical cell (or enclosed and protected material) that can be charged e for power or released electrical charge when needed.
Biometric Reader	A device that uses measurable biological characteristics such as fingerprints or iris

A comprehensive guide to the terminology used throughout the SIG

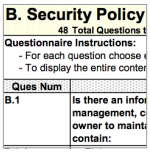
The Detail Tabs (A – Z)

Each of the detail tabs within the SIG allows the vendor to provide information on the extent of their risk controls within their environment.

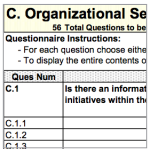
Please note: *There are a number of questions repeated in the SIG on different tabs. This is intentional. The SIG may be answered by different groups within the vendor's environment. The use of redundant questions facilitates the ability to validate the consistency of the risk controls provided.*


A. Risk Assessm
14 Total Questions
Questionnaire Instructions:
- For each question choose
- To display the entire cont
Ques Num
A.1
Is there a risk management, owner to main

TAB A: RISK MANAGEMENT is used to describe the vendor's risk assessment program. It is further used to assess the maturity and operating effectiveness of the program and provides insight into management's commitment to security and compliance, as well as their ability to make risk-based decisions.

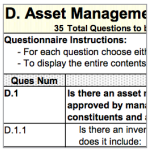

B. Security Policy
48 Total Questions t
Questionnaire Instructions:
- For each question choose
- To display the entire conte
Ques Num
B.1
Is there an info management, c owner to maint contain:

TAB B: SECURITY POLICY documents the information security policy controls of the responder's organization. Validating the existence of a comprehensive security policy provides assurance of the respondents overall approach to security.

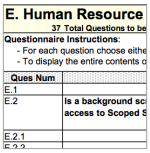

C. Organizational Se
56 Total Questions to be
Questionnaire Instructions:
- For each question choose eithe
- To display the entire contents o
Ques Num
C.1
Is there an informat initiatives within th
C.1.1
C.1.2
C.1.3

TAB C: ORGANIZATIONAL SECURITY assesses the structure and maturity of an organization's security function and its ability to meet its security obligations.

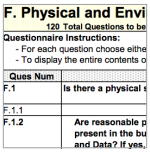
SHARED ASSESSMENTS


D. Asset Manageme
35 Total Questions to
Questionnaire Instructions:
- For each question choose eith
- To display the entire contents
Ques Num
D.1 Is there an asset approved by mana constituents and
D.1.1 Is there an inver does it include:

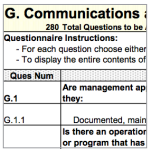
TAB D: ASSET MANAGEMENT determines whether the vendor has a formal asset management and classification structure in place to ensure that financial, security and privacy controls are effectively designed and operating properly.


E. Human Resource
37 Total Questions to be
Questionnaire Instructions:
- For each question choose eithe
- To display the entire contents
Ques Num
E.1
E.2 Is a background sc access to Scoped S
E.2.1

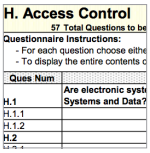
TAB E: HUMAN RESOURCE SECURITY documents whether the respondent has an HR security program in place that meets the personnel vetting and oversight requirements of the respondent's organization.


F. Physical and Envi
120 Total Questions to be
Questionnaire Instructions:
- For each question choose eithe
- To display the entire contents
Ques Num
F.1 Is there a physical
F.1.1
F.1.2 Are reasonable present in the bu and Data? If yes,

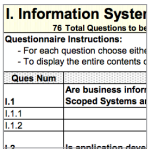
TAB F: PHYSICAL AND ENVIRONMENTAL SECURITY examines the organization's perimeter and first layer of defense in order to prevent unauthorized physical access, as well as accidental and intentional damage to the organizations' physical premises, systems and information. The Tab also looks at the steps taken to protect against environmental and systems malfunctions or failures.


G. Communications
280 Total Questions to be
Questionnaire Instructions:
- For each question choose either
- To display the entire contents of
Ques Num
G.1 Are management ap they:
G.1.1 Documented, main
Is there an operation or program that has

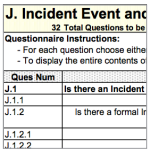
TAB G: COMMUNICATION AND OPERATIONS (OPS) MANAGEMENT conducts a detailed assessment of the operating procedures and technical controls used to ensure the effective management, operations, and integrity of the security information systems and data. A service provider's procedures for managing their third party vendors are also included in this tab.


H. Access Control
57 Total Questions to be
Questionnaire Instructions:
- For each question choose eithe
- To display the entire contents
Ques Num
H.1 Are electronic syst Systems and Data?
H.1.1
H.1.2
H.2

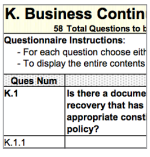
TAB H: ACCESS CONTROL examines the logical (technology-based) access controls of systems, password requirements, identity management, and controls placed around development, including access to information processing systems and facilities. In addition, it includes questions relating to remote access, encryption, and secure data transmission.


I. Information Syster
76 Total Questions to be
Questionnaire Instructions:
- For each question choose eithe
- To display the entire contents
Ques Num
I.1 Are business infor Scoped Systems a
I.1.1
I.1.2

TAB I: INFORMATION SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE (AD&M) examines the controls for application development, programming, data storage and transmission.

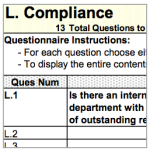

J. Incident Event and
32 Total Questions to be
Questionnaire Instructions:
- For each question choose eithe
- To display the entire contents
Ques Num
J.1 Is there an incident
J.1.1
J.1.2 Is there a formal
J.1.2.1

TAB J: INCIDENT EVENT AND COMMUNICATION MANAGEMENT looks to examine the respondent's incident management program, the ability of the company to respond effectively to an incident, and the maturity of the incident management program.

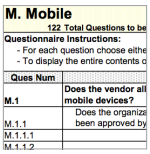

K. Business Contin
58 Total Questions to b
Questionnaire Instructions:
- For each question choose eith
- To display the entire contents
Ques Num
K.1 Is there a docume recovery that has appropriate const policy?
K.1.1

TAB K: BUSINESS CONTINUITY/DISASTER RECOVERY (BC/DR) determines if the respondent has incorporated business continuity considerations into the overall design of their business model, which are sufficient to mitigate the risk of service disruptions and supply chain failures. This tab examines whether technology, business operations, testing, and communication strategies critical to the renewal and continuation of services for the entire business are sufficiently addressed.

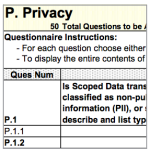
SHARED ASSESSMENTS


L. Compliance
13 Total Questions to
Questionnaire Instructions:
- For each question choose ei
- To display the entire content
Ques Num
L.1 Is there an intern department with of outstanding re
L.2

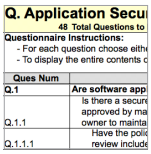
TAB L: COMPLIANCE examines the respondent's ability to satisfy requirements for data security and privacy protection consistent with the issuer's regulatory compliance obligations.


M. Mobile
122 Total Questions to be
Questionnaire Instructions:
- For each question choose eithe
- To display the entire contents c
Ques Num
M.1 Does the vendor all mobile devices?
M.1.1 Does the organiz been approved by
M.1.1.1
M.1.1.2

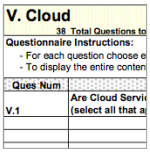
TAB M: MOBILE examines whether mobile devices are used to access the issuer's data and systems. If so, it examines the controls in place to manage mobile device use and access.


P. Privacy
50 Total Questions to be
Questionnaire Instructions:
- For each question choose either
- To display the entire contents of
Ques Num
P.1 Is Scoped Data trans classified as non-pu information (PII), or describe and list typ
P.1.1
P.1.2

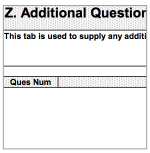
TAB P: PRIVACY examines the respondent's privacy program and privacy management framework used to protect the privacy of respondent's data through its full lifecycle of data collection, storage, usage, sharing, transferring, securing, retention, and destruction. In addition, this tab identifies any instances where issuer's data is obtained, transferred, moved, processed, or in any way leaves the U.S.


Q. Application Secu
48 Total Questions to
Questionnaire Instructions:
- For each question choose eith
- To display the entire contents c
Ques Num
Q.1 Are software app
Q.1.1 Is there a secur approved by ma owner to mainta
Q.1.1.1 Have the polic review include

TAB Q: APPLICATION SECURITY examines the respondent's process for developing software in a secure environment. The assessments of software application security primarily focuses on the formalized security processes implemented by the respondent.


V. Cloud
38 Total Questions to
Questionnaire Instructions:
- For each question choose e
- To display the entire conten
Ques Num
V.1 Are Cloud Servi (select all that a

TAB V: CLOUD question set of this tab is largely based on the Shared Assessments white paper, Evaluating Cloud Risk for the Enterprise: A Shared Assessments Guide. In this tab, the respondent identifies the service and deployment models used to provide Cloud services and the risk controls in place for each model.


Z. Additional Questior
This tab is used to supply any additi
Ques Num

TAB Z: ADDITIONAL QUESTIONS facilitates the ability of the issuer to provide additional questions unique to the services provided to them by the vendor.

OTHER TABS not referenced in this document include the Version History, Formula Notes and Full Tabs. The Full tab maps the questions in the SIG to relevant regulations and standards.

LEARN MORE

To learn more or to purchase the Shared Assessments Program Tools, or to obtain information about membership opportunities, contact Julie Lebo, Vice President Member Relations, The Santa Fe Group at **(703) 533-7256** or **julie@santa-fe-group.com.**