SFG | SHARED ASSESSMENTS
The Trusted Source in Third Party Risk Management

2019 SHARED ASSESSMENTS STANDARDIZED INFORMATION GATHERING (SIG) QUESTIONNAIRE TOOLS: SIG MANAGEMENT TOOL

The SIG Questionnaire Tools are a comprehensive questionnaire management interface that lets you build, customize, store and automatically analyze SIG questionnaires and their associated evidence requirements all in one place. It is built on a holistic set of industry best practices for gathering and assessing 18 critical control domains including information technology, cybersecurity, privacy, resiliency and compliance risks and their corresponding controls. Service providers can also use SIG Questionnaires to reduce assessment fatigue by proactively supplying their own SIGs to Outsourcers.

The Shared Assessments Program is administered by The Santa Fe Group (www.santa-fe-group.com). Questions about this workbook should be directed towards support@sharedassessments.org. If you are interested in the Shared Assessments Program and would like us to contact you, email us at info@sharedassessments.org.

Terms of Use

2019 SHARED ASSESSMENTS STANDARDIZED INFORMATION GATHERING (SIG) QUESTIONNAIRE TOOLS (2019 SIG)

The Shared Assessments Program ("Program") maintains, promotes and facilitates the use of the Standardized Information Gathering ("SIG") questionnaire documents and other Program resource documents.

The Shared Assessments Program attaches the following conditions to individuals and organizations downloading, copying and/or using the Program Documents:

- No modifications may be made to the Program documents without the express written permission of the Shared Assessments Program and The Santa Fe Group.
- Organizations must notify The Santa Fe Group at sharedassessments@santa-fe-group.com of their reasons for the modifications and make the modifications available for review and approval as additions and/or modifications to the current version of the documents.
- Copyright and all other intellectual property or proprietary rights in any modifications to the Shared Assessments Program documents shall belong to the Shared Assessments Program and The Santa Fe Group.
- Persons downloading the Program documents who wish to incorporate the SCA and/or SIG into a software product offered for license or sale must first obtain a separate license from the Shared Assessments Program.

The Program documents have been developed as tools for information security, privacy and business continuity compliance. They are based on general information security and privacy laws, regulation, principles, frameworks, audit programs, seal programs and regulatory guidance from various jurisdictions and do not constitute legal advice or an exhaustive list of questions or procedures covering all the information security or privacy laws in the US, or rest of the world, that may apply to a service provider. Each user should consult counsel on a case-by-case basis to ensure compliance with all applicable information security and privacy laws, regulations, policies and standards.

SFG | SHARED ASSESSMENTS
The Trusted Source in Third Party Risk Management

2019 SHARED ASSESSMENTS STANDARDIZED INFORMATION GATHERING (SIG) QUESTIONNAIRE
Version 2019
Released: 2019

The Shared Assessments Program
SIGIssues@sharedassessments.org

Issuer/Outsourcer Additional Information

Assessee Instructions

Filling out the SIG:
Review the instructions provided by your Issuer/Outsourcer on how to answer the SIG.
Issuer/Outsourcer should provide you with the scope of services for which to provide responses. The SIG is complex. If you did not receive instructions from your Issuer/Outsourcer it is recommended that you contact them before you start and seek guidance on how to proceed with the SIG to meet their needs.

Primary or 'parent' questions, indicated in bold, are followed by numbered sub or 'child' questions. If a parent question is answered Yes, child questions will display. There can be up to four generations of questions below a parent question. To display all of the questions (parent, child, grandchild, etc.) disable macros when opening the file or select Disable from the Tab Automation dropdown on each risk domain tab.

Steps:
1) Complete the Business Information tab.
2) Compile the documentation requested on the Documentation tab and update the tab with the documents provided.
3) Answer the questions in the displayed risk domain tabs as instructed by the Issuer/Outsourcer by selecting Yes, No, or N/A from the drop-down menu in the Response field.
4) Use the Additional Information field to provide any additional description, explanation, or information as needed. An explanation is recommended for N/A responses.
5) If available, choose a maturity level (1-5) from the Maturity drop-down field.

Note: There may be gaps in the question numbering depending on how the Issuer/Outsourcer scoped the SIG.

Dashboard

The Dashboard provides you with a quick and easy reference to determine the percentage of completion for the required sections of the SIG. As questions are answered, either directly or by being pre-filled, the Dashboard will track the completion percentage of each section.

Tabs	% Comp
Copyright	N/A
Terms of Use	N/A
Instructions	N/A
Business Information	15%
Documentation	N/A
A. Risk Assessment and Treatment	100%
B. Security Policy	100%
C. Organizational Security	100%
D. Asset and Information Management	100%
E. Human Resource Security	100%
F. Physical and Environmental Security	100%
G. Operations Management	100%
H. Access Control	100%
I. Application Security	100%
J. Incident Event and Communications Management	100%
K. Business Resiliency	95%
L. Compliance	100%
M. End User Device Security	100%
N. Network Security	100%
P. Privacy	100%
T. Threat Management	100%
U. Server Security	100%
V. Cloud Hosting	100%
Formula Notes	N/A
SIG Total	99%

Response Cell Background Color Coding (All tabs)	Resp
Response Required (cells with a gray background are editable)	
Yes Response	Yes
No Response	No
N/A Response	N/A
Top of table or Maturity not applicable (no response required)	

Business Information

Progress:	15%
Question/Request	
Assessee Name	
Assessee 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	Symantec Corporation
Company/business name	Symantec Corporation
Publicly or privately held company	Publicly held
If public, what is the name of the Exchange	NASDAQ
If public, what is the trading symbol	SYMC
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	
Has your company suffered a data loss or security breach within the last 3 years?	
If yes, please describe the loss or breach.	
Has any of your Third Party Vendors suffered a data loss or security breach within the last 3 years?	
If yes, please describe the loss or breach.	
Scope *Please provide the below responses to establish the scope of the SIG*	
Are the answers in this questionnaire for only one facility or geographic location? If yes, provide description of physical location (address, city, state, country).	
Backup site physical address	
Any additional locations where Scoped Systems and Data is stored	
If yes, provide each location (address, city, state, country).	
Are the answers to this questionnaire for only one specific type of service? If yes, describe the service.	Web Security Service (WSS)
Are software applications provided?	Yes
List the applications provided that are in scope.	
Identify the applications which are covered by the secure software development lifecycle.	
What type of software is being provided, select all that apply from the list below?	

Commercial Off-The-Shelf (COTS)	
Custom Developed	
Cloud	
Mobile	
Open Source Software	
Other	
Does your company require approval prior to submitting the responses and documentation associated with this document?	
If yes, describe your approval process and the individual who approves the submission.	
Does this SIG include Cloud Hosting services?	
What service hosting models are provided as part of this service?	
Data center: single tenancy?	
Co-location: dedicated server?	
Web Hosting?	
File Hosting?	
Continuous?	
Cloud Hosting: (e.g., AWS, Azure, Google, etc.)?	
What Cloud Hosting Tiers are provided as part of this service?	
Software as a Service (SaaS)?	
Infrastructure as a Service (IaaS)?	
What deployment models are provided (select all that apply):	
Private cloud?	
Public cloud?	
Community cloud?	
Hybrid cloud?	

Documentation*

Use this section to request any specific documentation you want the Assessee 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 to include the following (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 including network access. c) Documentation detailing execution of user entitlement reviews. d) Employee non-disclosure agreement. e) Incident report policy and procedures including all contract information. f) Copy of visitor policy and procedures. g) Log review policies and procedures. h) Third party risk management (TPRM) program policies and procedures.		
* Copy of internal or external audit report (e.g., SSAE18 SOC 2, ISO, HITRUST CSF, PCI ROC/SAQ attestation of compliance).		
Information technology and security organization charts (including where Assessee information security resides and the composition of any information security steering committees). **Note:** Names of employees should be redacted and Not included.		
* Physical Security policy and procedures (building and/or restricted access)		
* Third party security reviews/assessments/penetration tests.		
Legal clauses and confidentiality templates for third parties.		
Topics covered in the security training program.		
* Security incident handling and reporting process.		
Network configuration diagrams for internal and external networks defined in scope. **Note:** Sanitized versions of the network diagram are acceptable.		
* System and network configuration standards.		
* System backup policy and procedures.		
* Offsite storage policy and procedures.		
* Vulnerability and threat management scan policy and procedures.		
* Application security policy.		
* Change control policy/procedures.		
* Problem management policy/procedures.		
* Certification of proprietary encryption algorithms.		
* Internal vulnerability assessments results of systems, applications, and networks.		
* Software development and lifecycle (SDLC) process and procedures.		
* Business resiliency (business continuity and/or disaster recovery plan).		

* Most recent business resiliency test dates and results.		
* Most recent SCA (f.k.a AUP) final report.		
* Privacy Policies (internal, external, web).		
* Executive Summary of certificates held e.g. HIPAA, ISO.		
* Performance Reports against contracted SLAs.		

*If the Assessee policy prohibits the distribution of any of these documents, please provide the document title, the table of contents, the executive summary, revision history, and evidence of approval.

A. Risk Assessment and Treatment

Scoped As: SIG Core 2019 **Progress:** 100% **Tab Automation:** Enable

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 in column F to provide.
- To display the entire contents of the tab, select the word "Disable" in the Tab Automation field at the top of the page.
- Use the Maturity column to identify the Maturity of the question. See the How To Guide for instructions on filling out this field.

Note: There may be gaps in the question number sequence depending on how the issues/outsourcer generated the SIG.

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
A.1	**Is there a formalized risk governance plan and a continuous Risk Assessment program that identifies, quantifies, and prioritizes risks based on the risk acceptance levels relevant to the organization?**	Yes		IT & Infrastructure Risk Governance	Risk Governance Plan	A.1 IT and Infrastructure Risk Governance	6.1.2 Information Security Risk Asssessment
A.1.1	Does the risk governance plan include risk management policies, procedures, and internal controls?	Yes		IT & Infrastructure Risk Governance	Risk Governance Plan	A.1 IT and Infrastructure Risk Governance	6.1.2 Information Security Risk Asssessment
A.1.2	Does the risk governance plan include range of assets to include: people, processes, data and technology?	Yes		IT & Infrastructure Risk Governance	Risk Governance Plan	A.1 IT and Infrastructure Risk Governance A.2 IT and infrastructure Rick Assessment Life Cycle	6.1.2 Information Security Risk Asssessment
A.1.3	Does the risk governance plan include range of threats to include: malicious, natural, accidental, cyber, business changes (transaction volume)?	Yes		IT & Infrastructure Risk Governance	Risk Governance Plan	A.2 IT and infrastructure Rick Assessment Life Cycle	6.1.2 Information Security Risk Asssessment
A.1.4	Does the risk governance plan include risk scenarios including events and possible threats that could impact people, processes, technologies and facilities?	Yes		IT & Infrastructure Risk Governance	Risk Governance Plan	A.1 IT and Infrastructure Risk Governance A.2 IT and infrastructure Rick Assessment Life Cycle	6.1.2 Information Security Risk Asssessment
A.2.4	Are critical processes and entities reassessed annually?	Yes		IT & Infrastructure Risk Assessment Life Cycle	Risk Assessments	A.4 Risk Assessment Frequency	8.2 Information Security Risk Assessment
A.3	**Is there a program to manage the treatment of identified risks?**	Yes		IT & Infrastructure Risk Assessment Life Cycle	Risk Treatment	A.2 IT and infrastructure Rick Assessment Life Cycle	6.1.1 General 6.1.3 Information Security Risk Treatment 8.3 Information Security Risk Treatment
A.3.1	Does the program include a formal process for assigning appropriate management ownership for risk decisions?	Yes		IT & Infrastructure Risk Assessment Life Cycle	Risk Treatment	A.2 IT and infrastructure Rick Assessment Life Cycle	6.1.1 General 6.1.3 Information Security Risk Treatment 8.3 Information Security Risk Treatment
A.3.2	Does the program include a formal process for accepting risks and approving action plans?	Yes		IT & Infrastructure Risk Assessment Life Cycle	Risk Treatment	A.2 IT and infrastructure Rick Assessment Life Cycle	6.1.1 General 6.1.3 Information Security Risk Treatment 8.3 Information Security Risk Treatment
A.3.3	Does the program include a formal process for tracking the status of action plans and reporting them to management?	Yes		IT & Infrastructure Risk Assessment Life Cycle	Risk Treatment	A.2 IT and infrastructure Rick Assessment Life Cycle	6.1.1 General 6.1.3 Information Security Risk Treatment 8.3 Information Security Risk Treatment
A.3.4	Does the program include creation of internal controls if material risks are identified?	Yes		IT & Infrastructure Risk Assessment Life Cycle	Risk Treatment	A.2 IT and infrastructure Rick Assessment Life Cycle	6.1.1 General 6.1.3 Information Security Risk Treatment 8.3 Information Security Risk Treatment
A.3.5	Does the program include measures for defining, monitoring, and reporting risk metrics?	Yes		IT & Infrastructure Risk Assessment Life Cycle	Risk Reporting	A.2 IT and infrastructure Rick Assessment Life Cycle	6.1.1 General 6.1.3 Information Security Risk Treatment 8.3 Information Security Risk Treatment
A.4	**Do Subcontractors (e.g., backup vendors, service providers, equipment support maintenance, software maintenance vendors, data recovery vendors, hosting providers, etc.) have access to scoped systems and data or processing facilities?**	Yes		Third-Party Risk Management	Subcontractor Selection and Management Process	A.5 Third Party Provider Risk Management Program	

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
A.4.1	**Is there a documented third-party risk management program in place for the selection, oversight and risk assessment of subcontractors?**	Yes		Third-Party Risk Management	Subcontractor Selection and Management Process	A.7 Subcontractor Selection and Management Process	15.1.1 Information Security Policy for Supplier Relationships 15.2.1 Monitoring and Review of Supplier Services 15.2.2 Managing Changes to Supplier Services
A.4.1.2	Does the subcontractor third-party risk management program include assessments performed on all potential subcontractors before entering into contracts with them?	Yes		Third-Party Risk Management	Subcontractor Selection and Management Process	A.7 Subcontractor Selection and Management Process A.9 Documenting Information Security Assessments for Subcontractors	
A.4.1.8	Does the subcontractor third-party risk management program include notification of new or change in subcontractors?	Yes		Third-Party Risk Management	Subcontractor Selection and Management Process	A.7 Subcontractor Selection and Management Process	15.1.1 Information Security Policy for Supplier Relationships
A.4.1.9	Does the subcontractor third-party risk management program include defined procedures for subcontractor management?	Yes		Third-Party Risk Management	Subcontractor Selection and Management Process	A.7 Subcontractor Selection and Management Process	15.1.1 Information Security Policy for Supplier Relationships A.4.1.6
A.4.1.11	**Does the subcontractor third-party risk management program include review of Subcontractors' third-party risk program?**	Yes		Third-Party Risk Management	Subcontractors' Third-Party Risk Management	A.12 Subcontractor Information Security Policy and Standards	15.1.1 Information Security Policy for Supplier Relationships
A.4.1.11.1	Does the Subcontractor third-party risk management program include security review prior to engaging their services (logical, physical, other controls)?	Yes		Third-Party Risk Management	Subcontractors' Third-Party Risk Management		15.1.1 Information Security Policy for Supplier Relationships
A.4.1.13	Does the Subcontractor third-party risk management program include Confidentiality and/or Non Disclosure Agreement requirements?	Yes		Third-Party Risk Management	Subcontractors' Third-Party Risk Management	A.8 Subcontractor Contracting Process	
A.4.1.14	Does the Subcontractor risk management program include notification of changes affecting services rendered?	Yes		Third-Party Risk Management	Subcontractors' Third-Party Risk Management	A.9 Documenting Information Security Assessments for Subcontractors	15.2.2 Managing Changes to Supplier Services
A.4.1.15	**Does the Subcontractor risk management program include background checks performed for Service Provider Contractors and Subcontractors?**	Yes		Third-Party Risk Management	Service Provider Background Checks	E.1 Background Investigation Policy Content	
A.4.1.15.1	Are background checks performed at time of hire?	Yes		Third-Party Risk Management	Service Provider Background Checks	E.1 Background Investigation Policy Content	
A.4.1.15.2	Are background checks performed periodically?	Yes		Third-Party Risk Management	Service Provider Background Checks	E.1 Background Investigation Policy Content	
A.4.1.16	Are subcontractors evaluated for reassessment when risk posture, service offerings, or contract changes?	Yes		Third-Party Risk Management	Subcontractors' Third-Party Risk Management	A.9 Documenting Information Security Assessments for Subcontractors	
A.4.1.17	**Are there contracts with all subcontractors requiring assessment?**	Yes		Third-Party Risk Management	Service Provider Agreements	A.6 Service Provider Agreements A.8 Subcontractor Contracting Process	13.2.2 Agreements on Information Transfer 13.2.4 Confidentiality or Non-Disclosure Agreements 15.1.2 Addressing Security Within Supplier Agreements 15.1.3 Information and Communication Technology Supply Chain 16.1.3 Reporting Information Security Weaknesses 7.1.2 Terms and Condition of Employment 7.2.1 Management Responsibilities A.4.1.6

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
A.4.1.17.1	Do contracts with all subcontractors include Non-Disclosure/Confidentiality Agreements?	Yes		Third-Party Risk Management	Service Provider Agreements	A.6 Service Provider Agreements A.8 Subcontractor Contracting Process	13.2.2 Agreements on Information Transfer 13.2.4 Confidentiality or Non-Disclosure Agreements 15.1.2 Addressing Security Within Supplier Agreements 15.1.3 Information and Communication Technology Supply Chain 7.1.2 Terms and Condition of Employment
A.4.1.17.2	Do contracts with all subcontractors include ownership of information, trade secrets and intellectual property?	Yes		Third-Party Risk Management	Service Provider Agreements	A.8 Subcontractor Contracting Process	13.2.2 Agreements on Information Transfer 13.2.4 Confidentiality or Non-Disclosure Agreements 15.1.2 Addressing Security Within Supplier Agreements 15.1.3 Information and Communication Technology Supply Chain 7.1.2 Terms and Condition of Employment
A.4.1.17.3	Do contracts with all subcontractors include security requirements of products and services provided?	Yes		Third-Party Risk Management	Service Provider Agreements	A.6 Service Provider Agreements A.8 Subcontractor Contracting Process	13.2.2 Agreements on Information Transfer 15.1.2 Addressing Security Within Supplier Agreements 15.1.3 Information and Communication Technology Supply Chain 7.1.2 Terms and Condition of Employment
A.4.1.17.4	Do contracts with all subcontractors include permitted use of confidential information?	Yes		Third-Party Risk Management	Service Provider Agreements	A.6 Service Provider Agreements A.8 Subcontractor Contracting Process	13.2.2 Agreements on Information Transfer 15.1.2 Addressing Security Within Supplier Agreements 15.1.3 Information and Communication Technology Supply Chain 7.1.2 Terms and Condition of Employment
A.4.1.17.5	Do contracts with all subcontractors include data breach notification?	Yes		Third-Party Risk Management	Service Provider Agreements	A.6 Service Provider Agreements A.8 Subcontractor Contracting Process	13.2.2 Agreements on Information Transfer 15.1.2 Addressing Security Within Supplier Agreements 15.1.3 Information and Communication Technology Supply Chain 16.1.3 Reporting Information Security Weaknesses 7.1.2 Terms and Condition of Employment
A.4.1.17.7	Do contracts with all subcontractors include Right to audit?	No		Third-Party Risk Management	Service Provider Agreements	A.7 Subcontractor Selection and Management Process A.8 Subcontractor Contracting Process	15.1.2 Addressing Security Within Supplier Agreements 15.1.3 Information and Communication Technology Supply Chain 7.1.2 Terms and Condition of Employment A.4.1.6

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
A.4.1.17.8	Do contracts with all subcontractors include SLAs?	Yes		Third-Party Risk Management	Service Provider Agreements	A.8 Subcontractor Contracting Process	15.1.3 Information and Communication Technology Supply Chain 7.1.2 Terms and Condition of Employment A.4.1.6
A.4.1.17.9	Do contracts with all subcontractors include Indemnification/liability?	Yes		Third-Party Risk Management	Service Provider Agreements	A.6 Service Provider Agreements	15.1.2 Addressing Security Within Supplier Agreements 15.1.3 Information and Communication Technology Supply Chain 7.1.2 Terms and Condition of Employment
A.4.1.17.10	Do contracts with all subcontractors include termination/exit clause?	Yes		Third-Party Risk Management	Service Provider Agreements	A.8 Subcontractor Contracting Process	15.1.3 Information and Communication Technology Supply Chain 7.1.2 Terms and Condition of Employment
A.4.1.17.11	Do contracts with all subcontractors include breach of agreement terms?	Yes		Third-Party Risk Management	Service Provider Agreements	A.6 Service Provider Agreements A.8 Subcontractor Contracting Process	15.1.2 Addressing Security Within Supplier Agreements 15.1.3 Information and Communication Technology Supply Chain 7.1.2 Terms and Condition of Employment
A.4.1.17.13	Do contracts with all subcontractors include security control requirements for subcontractors?	Yes		Third-Party Risk Management	Service Provider Agreements	A.12 Subcontractor Information Security Policy and Standards	13.2.2 Agreements on Information Transfer 15.1.2 Addressing Security Within Supplier Agreements 15.1.3 Information and Communication Technology Supply Chain 7.1.2 Terms and Condition of Employment 7.2.1 Management Responsibilities
A.4.2	**Is there a third party risk management program with an assigned individual or group responsible for capturing, maintaining and tracking subcontractor Information Security issues?**	Yes		Third-Party Risk Management	Continuous Monitoring	A.5 Third Party Provider Risk Management Program	
A.4.2.6	Does the remediation reporting include a process to identify and log subcontractor information security, privacy and/or data breach issues?	Yes		Third-Party Risk Management	Continuous Monitoring	A.1 IT and Infrastructure Risk Governance	12.4.1 Event Logging

B. Security Policy

Scoped As: SIG Core 2019 **Progress:** 100% **Tab Automation:** Enable

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 in column F to provide.
- To display the entire contents of the tab, select the word "Disable" in the Tab Automation field at the top of the page.
- Use the Maturity column to identify the Maturity of the question. See the How To Guide for instructions on filling out this field.

Note: There may be gaps in the question number sequence depending on how the issues/outsourcer generated the SIG.

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
B.1	**Is there a set of information security policies that have been approved by management, published and communicated to constituents?**	Yes		Information Security Policy Management	Information Security Policy Management	B.1 Information Security Policy Maintenance	4.3 Scope of Information Security Management Systems 5.1 Leadership and Commitment 5.1.1 Policies for Information Security 5.2 Policy 6.2 Information Security Objectives and Planning to Achieve Them 7.4 Communication 7.5.1 General 8.1 Operational Planning and Control
B.1.1	Are policies and standards based on industry accepted standards and practices?	Yes		Information Security Policy Management	Information Security Policy Management	B.1 Information Security Policy Maintenance B.2 Information Security Standards	6.2 Information Security Objectives and Planning to Achieve Them
B.1.2	Is there a management-approved process for handling deviations and exceptions?	Yes		Information Security Policy Management	Information Security Policy Management	B.2 Information Security Standards	6.2 Information Security Objectives and Planning to Achieve Them
B.1.3	Do the information security policies set requirements based on business strategy, regulations, legislation (Including Privacy and civil liberties obligations) and cybersecurity threat environment?	Yes		Information Security Policy Management	Information Security Policy Management		4.3 Scope of Information Security Management Systems 6.2 Information Security Objectives and Planning to Achieve Them 8.1 Operational Planning and Control
B.1.5	**Have all policies been assigned to an owner responsible for review and approve periodically?**	Yes		Information Security Policy Management	Information Security Policy Management	B.2 Information Security Standards	4.4 Information Security Management System 6.2 Information Security Objectives and Planning to Achieve Them 9.1 Monitoring, Measurement, Analysis, and Evaluation 9.3 Management Review
B.1.5.1	Do owners review and update policies if significant changes occur in legal, business, organizational, or technical conditions?	Yes		Information Security Policy Management	Information Security Policy Management	B.2 Information Security Standards	10.2 Continual Improvement 4.4 Information Security Management System 5.1.2 Review of the Policies for Information Security 9.1 Monitoring, Measurement, Analysis, and Evaluation 9.3 Management Review
B.1.6	Have all information security policies and standards been reviewed in the last 12 months?	Yes		Information Security Policy Management	Information Security Policy Management	B.2 Information Security Standards	10.2 Continual Improvement 4.4 Information Security Management System 5.1.2 Review of the Policies for Information Security 9.1 Monitoring, Measurement, Analysis, and Evaluation 9.3 Management Review

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
B.2	Is the maturity of IT management processes formally evaluated at least annually using an established benchmark (e.g., COBIT maturity models)?	Yes		IT Governance	Maturity Benchmarking		10.2 Continual Improvement 9.1 Monitoring, Measurement, Analysis, and Evaluation

C. Organizational Security

Scoped As: SIG Core 2019 **Progress:** 100% **Tab Automation:** Enable

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 in column F to provide.
- To display the entire contents of the tab, select the word "Disable" in the Tab Automation field at the top of the page.
- Use the Maturity column to identify the Maturity of the question. See the How To Guide for instructions on filling out this field.

Note: There may be gaps in the question number sequence depending on how the issues/outsourcer generated the SIG.

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
C.1	**Are responsibilities for asset protection and for carrying out specific information security processes clearly identified and communicated to the relevant parties?**	Yes		Organizational Security	Organizational Information Security Responsibilities	C.1 Security Organization Roles and Responsibilities	5.3 Organizational Roles, Responsibilities, and Authorities 6.1.1 Information Security Roles and Responsibilities
C.1.1	Do the processes include residual risk acceptance responsibilities?	Yes		Organizational Security	Organizational Information Security Responsibilities	C.1 Security Organization Roles and Responsibilities	5.3 Organizational Roles, Responsibilities, and Authorities 6.1.1 Information Security Roles and Responsibilities
C.2	Do all projects involving Scoped Systems and Data go through some form of information security assessment?	Yes		Organizational Security	Project Information Security Assessment		6.1.5 Information Security in Project Management
C.3	**Are information security personnel (internal or outsourced) responsible for information security processes?**	Yes		Organizational Security	Information Security Personnel Responsibilities	C.1 Security Organization Roles and Responsibilities	10.1 Nonconformity and Corrective Action Plan 10.2 Continual Improvement 4.1 Understanding Organization and its Context 4.3 Scope of Information Security Management Systems 4.4 Information Security Management System 6.2 Information Security Objectives and Planning to Achieve Them 7.1 Resources 8.1 Operational Planning and Control 9.1 Monitoring, Measurement, Analysis, and Evaluation
C.3.1	Are information security personnel responsible for the design of information technology systems, processes, and architecture required to meet information security requirements?	Yes		Organizational Security	Information Security Personnel Responsibilities	I.8 Secure Architectural Design Standards U.1 System Configuration and Hardening Standards	18.2.3 Technical Compliance Review 4.1 Understanding Organization and its Context 4.3 Scope of Information Security Management Systems 4.4 Information Security Management System 6.2 Information Security Objectives and Planning to Achieve Them 7.1 Resources 8.1 Operational Planning and Control

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
C.3.2	Are information security personnel responsible for the creation, and review of information security policies?	Yes		Organizational Security	Information Security Personnel Responsibilities	B.2 Information Security Standards	10.2 Continual Improvement 4.1 Understanding Organization and its Context 4.3 Scope of Information Security Management Systems 4.4 Information Security Management System 6.2 Information Security Objectives and Planning to Achieve Them 7.1 Resources 8.1 Operational Planning and Control 9.1 Monitoring, Measurement, Analysis, and Evaluation
C.3.3	Do information security personnel review the effectiveness of information security policy implementation and manage instances of non-compliance with security policies across the entire organization?	Yes		Organizational Security	Information Security Personnel Responsibilities	B.2 Information Security Standards	10.1 Nonconformity and Corrective Action Plan 10.2 Continual Improvement 18.2.3 Technical Compliance Review 4.1 Understanding Organization and its Context 4.4 Information Security Management System 6.2 Information Security Objectives and Planning to Achieve Them 7.1 Resources 8.1 Operational Planning and Control 9.1 Monitoring, Measurement, Analysis, and Evaluation
C.3.5	Are information security personnel responsible for the monitoring of significant changes in the exposure of information assets?	Yes		Organizational Security	Information Security Personnel Responsibilities	A.2 IT and infrastructure Rick Assessment Life Cycle	4.4 Information Security Management System 6.2 Information Security Objectives and Planning to Achieve Them 7.1 Resources 9.1 Monitoring, Measurement, Analysis, and Evaluation
C.3.6	Are information security personnel responsible for the review and/or monitoring information security incidents or events?	Yes		Organizational Security	Information Security Personnel Responsibilities	I.17 System Monitoring J.5 IS/IT Incident Management – Detection	4.4 Information Security Management System 6.2 Information Security Objectives and Planning to Achieve Them 7.1 Resources 9.1 Monitoring, Measurement, Analysis, and Evaluation
C.4	**Has a qualified individual responsible been designated as a Chief Information Security Officer (CISO) to oversee and implement the organization's cybersecurity program and enforce its cybersecurity policy?**	Yes		NYDFS Cybersecurity Regulation (23 NYCRR 500)	Chief Information Security Officer		
C.4.1	Does the CISO issue a report at least annually on the organization's cybersecurity program and material cybersecurity risks to the organization's board of directors, equivalent body, or senior officer in charge of cybersecurity risk?	Yes		NYDFS Cybersecurity Regulation (23 NYCRR 500)	Chief Information Security Officer		
C.5	Do information security personnel maintain professional security certifications?	Yes		Organizational Security	Information Security Personnel Qualifications	C.1 Security Organization Roles and Responsibilities	7.2 Competence

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
C.6	Do information security personnel maintain contacts with information security special interest groups, specialist security forums or professional associations?	Yes		Organizational Security	Information Security Personnel Qualifications	C.1 Security Organization Roles and Responsibilities	6.1.4 Contact with Special Interest Groups 7.2 Competence
C.7	Do Information security personnel participate in continuing education programs (e.g., online training, webinars, seminars, etc.)?	Yes		Organizational Security	Information Security Personnel Qualifications		7.2 Competence

D. Asset and Information Management

Scoped As: SIG Core 2019 **Progress:** 100% **Tab Automation:** Enable

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 in column F to provide.
- To display the entire contents of the tab, select the word "Disable" in the Tab Automation field at the top of the page.
- Use the Maturity column to identify the Maturity of the question. See the How To Guide for instructions on filling out this field.

Note: There may be gaps in the question number sequence depending on how the issues/outsourcer generated the SIG.

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
D.1	**Is there an asset management program approved by management, communicated to constituents and an owner to maintain and review?**	Yes		Asset Management	Asset Inventory	D.1 Asset Accounting and Inventory	8.1.1 Inventory of Assets
D.1.1	**Is there an asset Inventory list or configuration management Database (CMDB)?**	Yes		Asset Management	Asset Inventory	D.1 Asset Accounting and Inventory	8.1.1 Inventory of Assets
D.1.1.1	Is the asset inventory updated on a periodic basis as new system assets are connected to the network?	Yes		Asset Management	Asset Inventory	D.1 Asset Accounting and Inventory	8.1.1 Inventory of Assets
D.1.1.2	Are machine name, unique Identification number, purpose, asset owner, Operating System, physical location, Business Function/Department, Environment (PROD, Dev, Test etc.) documented for all devices on the network?	Yes		Asset Management	Asset Inventory	D.1 Asset Accounting and Inventory	7.5.1 General 7.5.2 Creating and Updating 8.1.1 Inventory of Assets
D.1.1.3	Is Environment (Development, Test, etc.) documented for all devices on the network?	Yes		Asset Management	Asset Inventory	D.1 Asset Accounting and Inventory	7.5.2 Creating and Updating 8.1.1 Inventory of Assets
D.1.1.4	Are all installed software platforms and applications on Scoped Systems inventoried?	Yes		Asset Management	Asset Inventory	D.1 Asset Accounting and Inventory	7.5.2 Creating and Updating 8.1.1 Inventory of Assets
D.1.1.5	Is data classification documented for all assets?	Yes		Asset Management	Asset Inventory	D.1 Asset Accounting and Inventory	7.5.2 Creating and Updating 8.1.1 Inventory of Assets
D.1.2	Is an Automated asset inventory discovery tool used to inventory devices on the network?	Yes		Asset Management	Automated Asset Inventory		8.1.1 Inventory of Assets
D.2	**Is there an acceptable use policy for information and associated assets that has been approved by management, communicated to appropriate Constituents and assigned an owner to maintain and periodically review the policy?**	Yes		Asset Management	Acceptable Use	E.2 Agreements for Constituents	8.1.3 Acceptable Use of Assets
D.2.1	Are Constituents made aware of and held accountable to the Acceptable Use Policy?	Yes		Asset Management	Acceptable Use	E.2 Agreements for Constituents	8.1.3 Acceptable Use of Assets
D.3	Is there a process to verify return of constituent assets (computers, cell phones, access cards, tokens, smart cards, keys, etc.) upon termination?	Yes		Asset Management	Asset Recovery		8.1.4 Return of Assets
D.4	**Is Information classified according to legal or regulatory requirements, business value, and sensitivity to unauthorized disclosure or modification?**	Yes		Information Management	Information Classification	D.1 Asset Accounting and Inventory	8.2.1 Classification of Information
D.4.1	Is information reclassified as information value, sensitivity, and customer requirements change?	Yes		Information Management	Information Classification	D.1 Asset Accounting and Inventory	8.2.1 Classification of Information
D.4.3	**Is an owner assigned to all Information Assets?**	Yes		Information Management	Information Ownership	D.1 Asset Accounting and Inventory	8.1.2 Ownership of Assets
D.4.3.1	Are owners responsible to ensure their Information Assets are inventoried, appropriately classified, protected, and decommissioned properly?	Yes		Information Management	Information Ownership	D.1 Asset Accounting and Inventory	8.1.2 Ownership of Assets
D.4.3.2	Are owners responsible to approve and periodically review access to Information Assets?	Yes		Information Management	Information Ownership	B.2 Information Security Standards H.3 Logical Access Authorization	8.1.2 Ownership of Assets 9.2.5 Review of User Access Rights
D.4.4	**Is there a policy or procedure for information handling (storing, processing, and communicating) consistent with its classification that has been approved by management, communicated to appropriate constituents and assigned an owner to maintain and periodically review?**	Yes		Information Management	Information Handling	D.1 Asset Accounting and Inventory	10.1.1 Policy on the Use of Cryptographic Controls 14.1.2 Securing Application Services on Public Networks 7.5.3 Control of Documented Information 8.2.2 Labelling of Information 8.2.3 Handing of Assets 8.3.1 Management of Removable Media

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
D.4.4.1	Does the policy or procedure for information handling include access control requirements including restrictions and authorized parties?	Yes		Information Management	Information Handling	B.2 Information Security Standards	10.1.1 Policy on the Use of Cryptographic Controls 7.5.3 Control of Documented Information 8.2.3 Handing of Assets
D.4.4.2	Does the policy or procedure for information handling include encryption requirements?	Yes		Information Management	Information Handling	D.5 Data Security Policy - Encryption	10.1.1 Policy on the Use of Cryptographic Controls 7.5.3 Control of Documented Information 8.2.3 Handing of Assets
D.4.4.3	Does the policy or procedure for information handling include storage requirements including authorized use of Public Cloud storage?	Yes		Information Management	Information Handling	D.5 Data Security Policy - Encryption	7.5.3 Control of Documented Information 8.2.3 Handing of Assets
D.4.4.4	Does the policy or procedure for information handling include electronic transmission security requirements including email, web, and file transfer services?	Yes		Information Management	Information Handling	D.5 Data Security Policy - Encryption	13.2.3 Electronic Messaging 7.5.3 Control of Documented Information 8.2.3 Handing of Assets
D.4.4.5	Does the policy or procedure for information handling include removable media (Thumb Drives, DVDs, Tapes, etc.) requirements?	Yes		Information Management	Information Handling	D.4 Removable Device Security	7.5.3 Control of Documented Information 8.2.3 Handing of Assets 8.3.1 Management of Removable Media
D.4.4.6	Does the policy or procedure for information handling ensure information's classification is properly labeled in its related physical and electronic formats?	Yes		Information Management	Information Handling	D.1 Asset Accounting and Inventory	7.5.3 Control of Documented Information 8.2.2 Labelling of Information 8.2.3 Handing of Assets
D.4.5	Is there a data retention/destruction requirement that includes information on live media, backup/archived media, and information managed by Subcontractors?	Yes		Information Management	Information Handling	D.1 Asset Accounting and Inventory	7.5.3 Control of Documented Information
D.4.6	**Is all media containing Scoped Data disposed of securely?**	Yes		Media Security	Media Disposal	D.8 Asset Destruction and Disposal	11.2.7 Secure Disposal and Re-use of Equipment 8.3.2 Disposal of Media
D.4.6.1	If in electronic form, is all Scoped Data made unrecoverable (wiped or overwritten) prior to asset reuse?	Yes		Media Security	Media Disposal	D.8 Asset Destruction and Disposal	11.2.7 Secure Disposal and Re-use of Equipment 8.3.2 Disposal of Media
D.4.6.2	Is media disposal logged to maintain an audit trail?	Yes		Media Security	Media Disposal	D.8 Asset Destruction and Disposal	12.4.1 Event Logging 8.3.2 Disposal of Media
D.5	**Is Scoped Data sent or received via physical media?**	No		Physical Media Transmission	Physical Media Transport Integrity	D.2 Physical Media Tracking	13.2.1 Information Transfer Policies and Procedures 8.3.3 Physical Media Transfer
D.5.1	Do transport containers protect against physical damage?	N/A		Physical Media Transmission	Physical Media Transport Integrity	D.2 Physical Media Tracking	13.2.1 Information Transfer Policies and Procedures 8.3.3 Physical Media Transfer
D.5.2	Are Locked or tamper evident transport containers used to transport Scoped Data?	N/A		Physical Media Transmission	Physical Media Transport Integrity	D.2 Physical Media Tracking	13.2.1 Information Transfer Policies and Procedures 8.3.3 Physical Media Transfer
D.5.3	Are chain of custody logs identifying media contents, protection applied, times of transfer and receipt at destination used when transporting Scoped Data?	N/A		Physical Media Transmission	Physical Media Transport Integrity	D.2 Physical Media Tracking	12.4.1 Event Logging 13.2.1 Information Transfer Policies and Procedures 7.5.1 General 8.3.3 Physical Media Transfer
D.6	**Is Scoped Data sent or received electronically?**	Yes		Data Transmission	Data Transmission Security Policy	D.5 Data Security Policy - Encryption	10.1.1 Policy on the Use of Cryptographic Controls 13.2.1 Information Transfer Policies and Procedures 13.2.2 Agreements on Information Transfer 13.2.3 Electronic Messaging

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
D.6.1	Are policies, procedures, and controls for transferring information enforced?	Yes		Data Transmission	Data Transmission Security Policy	D.5 Data Security Policy - Encryption	13.2.1 Information Transfer Policies and Procedures 13.2.2 Agreements on Information Transfer 13.2.3 Electronic Messaging
D.6.2	Is all Scoped Data sent or received electronically encrypted in transit while outside the network?	Yes		Data Transmission	Data Transmission Security Policy - Encryption	D.5 Data Security Policy - Encryption	10.1.1 Policy on the Use of Cryptographic Controls 13.2.1 Information Transfer Policies and Procedures 13.2.3 Electronic Messaging
D.6.4	Does all Scoped Data sent or received electronically include encryption of e-mail, chat and other messaging technologies?	Yes		Data Transmission	Data Transmission Security Policy - Encryption	D.5 Data Security Policy - Encryption	10.1.1 Policy on the Use of Cryptographic Controls 13.2.1 Information Transfer Policies and Procedures 13.2.3 Electronic Messaging 14.1.2 Securing Application Services on Public Networks
D.6.5	Does Scoped Data sent or received electronically include content filtering scans performed on incoming/outgoing email to enforce email policy?	Yes		Data Transmission	Data Transmission Security Policy - Traffic Filtering		13.2.1 Information Transfer Policies and Procedures 13.2.3 Electronic Messaging 14.1.2 Securing Application Services on Public Networks
D.6.6	Does Scoped Data sent or received electronically include protection against malicious code by network virus inspection or virus scan at the endpoint?	Yes		Data Transmission	Data Transmission Security Policy - Traffic Filtering	T.2 Virus Protection (Servers)	13.2.1 Information Transfer Policies and Procedures 13.2.3 Electronic Messaging 14.1.2 Securing Application Services on Public Networks
D.6.7	Do scans performed on incoming and outgoing email include phishing prevention?	Yes		Data Transmission	Phishing Prevention	D.5 Data Security Policy - Encryption	10.1.1 Policy on the Use of Cryptographic Controls
D.6.9	**Is regulated or confidential Scoped Data stored electronically?**	Yes		Encryption	Scoping	D.5 Data Security Policy - Encryption	10.1.1 Policy on the Use of Cryptographic Controls
D.6.9.1	Is full-disk encryption enabled for all systems that store or process Scoped Data?	Yes		Encryption	Disk Encryption	D.5 Data Security Policy - Encryption	10.1.1 Policy on the Use of Cryptographic Controls
D.6.10	**Is regulated or confidential Scoped Data stored in a database?**	Yes		Encryption	Database Encryption	D.5 Data Security Policy - Encryption	10.1.1 Policy on the Use of Cryptographic Controls
D.6.10.1	Does regulated or confidential Scoped Data stored in a database include Database encryption?	Yes		Encryption	Database Encryption	D.5 Data Security Policy - Encryption	10.1.1 Policy on the Use of Cryptographic Controls
D.6.11	**Is regulated or confidential Scoped Data stored in files?**	Yes		Encryption	File/Folder Encryption	D.5 Data Security Policy - Encryption	10.1.1 Policy on the Use of Cryptographic Controls
D.6.11.1	Does regulated or confidential Scoped Data stored in files include file/folder-level encryption enabled?	Yes		Encryption	File/Folder Encryption	D.5 Data Security Policy - Encryption	10.1.1 Policy on the Use of Cryptographic Controls
D.6.12	**Are encryption keys managed and maintained for Scoped Data?**	Yes		Encryption	Key Management	D.5 Data Security Policy - Encryption	10.1.1 Policy on the Use of Cryptographic Controls 10.1.2 Key Management 6.1.2 Segregation of Duties
D.6.12.1	Are the encryption keys generated in a manner consistent with key management industry standards?	Yes		Encryption	Key Management	D.5 Data Security Policy - Encryption	10.1.1 Policy on the Use of Cryptographic Controls 10.1.2 Key Management
D.6.12.2	Are encryption keys encrypted at rest and when transmitted?	Yes		Encryption	Key Management	D.5 Data Security Policy - Encryption	10.1.1 Policy on the Use of Cryptographic Controls 10.1.2 Key Management
D.6.12.3	Is there segregation of duties between personnel responsible for key management duties and those responsible for normal operational duties?	Yes		Encryption	Key Management	D.5 Data Security Policy - Encryption	10.1.1 Policy on the Use of Cryptographic Controls 10.1.2 Key Management 6.1.2 Segregation of Duties
D.6.12.5	Is there a centralized key management system (KMS)?	Yes		Encryption	Key Management	D.5 Data Security Policy - Encryption	10.1.1 Policy on the Use of Cryptographic Controls 10.1.2 Key Management

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
D.6.12.6	Is the use of keys by personnel logged?	Yes		Encryption	Key Management	I.14 Web Server and Application Log on Activity Logging I.15 Administrative Activity Logging	10.1.1 Policy on the Use of Cryptographic Controls 10.1.2 Key Management 12.4.1 Event Logging
D.6.12.7	Does key generation and management occur in a software solution? (e.g., bouncycastle, OpenSSL)	Yes		Encryption	Key Management	D.5 Data Security Policy - Encryption	10.1.1 Policy on the Use of Cryptographic Controls 10.1.2 Key Management
D.6.12.8	Does key generation and management occur in a hardware Encryption Module (hardware Security Module) (e.g., NIST FIPS 140 2)?	Yes		Encryption	Key Management	D.5 Data Security Policy - Encryption	10.1.1 Policy on the Use of Cryptographic Controls 10.1.2 Key Management
D.6.13	Is there an option for clients to manage their own encryption keys?	No		Encryption	Key Management		10.1.1 Policy on the Use of Cryptographic Controls
D.6.14	**Is Asymmetric encryption key length a minimum of 2048 bits?**	Yes		Encryption	Cryptographic Strength	D.5 Data Security Policy - Encryption	10.1.1 Policy on the Use of Cryptographic Controls
D.6.14.1	Does Symmetric encryption use AES with a key length of at least 128 bits?	Yes		Encryption	Cryptographic Strength	D.5 Data Security Policy - Encryption	10.1.1 Policy on the Use of Cryptographic Controls
D.7	**Are Constituents able to view client's unencrypted Data?**	No		Encryption	Constituent Access		
D.7.1	Do Constituents have the ability to view an unencrypted version of regulated or confidential Information?	N/A		Encryption	Constituent Access		
D.8	Can Clients specify where their data is stored (logically and physically)?	Yes		Client Data Segmentation	Information Storage Location	V.1 Service and Deployment Models	
D.9	**Is data segmentation and separation capability between clients provided?**	Yes		Client Data Segmentation	Data Segmentation	V.1 Service and Deployment Models	
D.9.6	Does data segmentation and separation include Database segmentation (i.e. separate database instance for each client)?	Yes		Client Data Segmentation	Database Segmentation		
D.10	In the event of a subpoena or forensics incident, is specific data able to be put on Litigation Hold without impacting other clients' data?	Yes		Client Data Segmentation	E-Discovery and Litigation Hold	J.6 IS/IT Incident Management – Analysis	

E. Human Resource Security

Scoped As: SIG Core 2019 **Progress:** 100% **Tab Automation:** Enable

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 in column F to provide.
- To display the entire contents of the tab, select the word "Disable" in the Tab Automation field at the top of the page.
- Use the Maturity column to identify the Maturity of the question. See the How To Guide for instructions on filling out this field.

Note: There may be gaps in the question number sequence depending on how the issues/outsourcer generated the SIG.

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
E.1	**Are Human Resource policies approved by management, communicated to Constituents and an owner to maintain and review?**	Yes		Human Resource Policy	Human Resource Policy	E.1 Background Investigation Policy Content	7.2 Competence 7.2.1 Management Responsibilities 7.2.3 Disciplinary Process 7.3 Awareness 7.3.1 Termination or Change of Employment Responsibilities
E.1.1	**Do Human Resource policies include Constituent background screening criteria?**	Yes		Human Resource Policy	Background Investigation Policy Content	E.1 Background Investigation Policy Content	7.1.1 Screening 7.2 Competence
E.1.1.1	Does Constituent background screening criteria include Criminal screening?	Yes		Human Resource Policy	Background Investigation Policy Content	E.1 Background Investigation Policy Content	7.1.1 Screening
E.1.1.2	Does Constituent background screening criteria include Credit checks?	Yes		Human Resource Policy	Background Investigation Policy Content	E.1 Background Investigation Policy Content	7.1.1 Screening
E.1.1.4	Does Constituent background screening criteria include Reference verification?	Yes		Human Resource Policy	Background Investigation Policy Content	E.1 Background Investigation Policy Content	7.1.1 Screening 7.2 Competence
E.1.1.5	Does Constituent background screening criteria include Resume or curriculum vitae verification?	Yes		Human Resource Policy	Background Investigation Policy Content	E.1 Background Investigation Policy Content	7.1.1 Screening 7.2 Competence
E.1.2	**Are Constituents required to sign employment agreements?**	Yes		Human Resource Policy	Agreements for Constituents	E.2 Agreements for Constituents	7.1.2 Terms and Condition of Employment 7.2.1 Management Responsibilities
E.1.2.1	Do employment agreements include Acknowledgement of Acceptable Use policies?	Yes		Human Resource Policy	Agreements for Constituents	E.2 Agreements for Constituents	7.1.2 Terms and Condition of Employment 7.2.1 Management Responsibilities
E.1.2.2	Do employment agreements include acknowledgement of Code of Conduct / Ethics policies?	Yes		Human Resource Policy	Agreements for Constituents	E.2 Agreements for Constituents	7.1.2 Terms and Condition of Employment 7.2.1 Management Responsibilities
E.1.2.3	Do employment agreements include acknowledgement of Confidentiality / Non-Disclosure policies?	Yes		Human Resource Policy	Agreements for Constituents	E.2 Agreements for Constituents	7.1.2 Terms and Condition of Employment 7.2.1 Management Responsibilities
E.1.3	**Are Constituents required to attend security awareness training?**	Yes		Human Resource Policy	Security Awareness Training Program	E.3 Security Awareness Training Program	16.1.3 Reporting Information Security Weaknesses 7.2 Competence 7.2.1 Management Responsibilities 7.2.2 Information Security Awareness, Education and Training 7.3 Awareness

E.1.3.1	Does the security awareness training program include security policies, procedures and processes?	Yes		Human Resource Policy	Security Awareness Training Program	E.3 Security Awareness Training Program	16.1.3 Reporting Information Security Weaknesses 7.2 Competence 7.2.1 Management Responsibilities 7.2.2 Information Security Awareness, Education and Training 7.3 Awareness
E.1.3.2	Does the security awareness training program include techniques to recognize phishing attempts?	Yes		Human Resource Policy	Security Awareness Training Program		
E.1.3.3	Does the security awareness training program include an explanation of Constituents' security roles and responsibilities?	Yes		Human Resource Policy	Security Awareness Training Program	E.3 Security Awareness Training Program	16.1.3 Reporting Information Security Weaknesses 7.2 Competence 7.2.1 Management Responsibilities 7.2.2 Information Security Awareness, Education and Training 7.3 Awareness
E.1.3.5	Does the security awareness training program include new hire and annual participation?	Yes		Human Resource Policy	Security Awareness Training Program	E.3 Security Awareness Training Program	7.2 Competence 7.2.1 Management Responsibilities 7.2.2 Information Security Awareness, Education and Training 7.3 Awareness
E.1.4	Does the Human Resource policy include a disciplinary process for non-compliance?	Yes		Human Resource Policy	Disciplinary Process	E.3 Security Awareness Training Program	7.2.1 Management Responsibilities 7.2.3 Disciplinary Process 7.3 Awareness
E.1.5	Does the Human Resource policy include Constituent accountability for the use and misuse of their access credentials?	Yes		Human Resource Policy	Disciplinary Process	E.2 Agreements for Constituents	7.2.1 Management Responsibilities
E.1.6	Does the Human Resource policy include Termination and/or change of status processes?	Yes		Human Resource Policy	Separation Procedures	E.5 Separation Procedures	7.3.1 Termination or Change of Employment Responsibilities
E.2	Is electronic access to systems containing scoped data removed within 24 hours for terminated constituents?	Yes		Human Resource Policy	Separation Procedures	E.5 Separation Procedures H.2 Revoke System and Physical Access	9.2.6 Removal or Adjustment of Access Rights

F. Physical and Environmental Security

Scoped As: SIG Core 2019 **Progress:** 100% **Tab Automation:** Enable

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 in column F to provide.
- To display the entire contents of the tab, select the word "Disable" in the Tab Automation field at the top of the page.
- Use the Maturity column to identify the Maturity of the question. See the How To Guide for instructions on filling out this field.

Note: There may be gaps in the question number sequence depending on how the issues/outsourcer generated the SIG.

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
F.1	**Is there a physical security program approved by management, communicated to constituents, and has an owner been assigned to maintain and review?**	Yes		Physical Security Program	Physical Security Controls - Scoped Data	F.2 Physical Security Controls	11.1.3 Securing Offices, Rooms, and Facilities 11.1.5 Working in Secure Areas 11.2.9 Clear Desk and Clear Screen Policy
F.1.1	Does the physical security program include physical access and environmental controls?	Yes		Physical Security Program	Physical Security Controls - Scoped Data	F.1 Environmental Controls F.2 Physical Security Controls	11.1.3 Securing Offices, Rooms, and Facilities 11.1.5 Working in Secure Areas
F.1.2	Does the physical security program include a clean desk policy?	Yes		Physical Security Program	Secure Workspace Program	F.3 Secure Workspace Program	11.1.3 Securing Offices, Rooms, and Facilities 11.1.5 Working in Secure Areas 11.2.9 Clear Desk and Clear Screen Policy
F.1.3	Does the physical security program include signage to identify the data center?	Yes		Physical Security Program	Secure Workspace Perimeter	F.2 Physical Security Controls	11.1.3 Securing Offices, Rooms, and Facilities
F.1.4	**Are there physical security and environmental controls in the data center and office buildings?**	Yes		Physical Security Program	Physical Security Controls - Scoped Data	F.1 Environmental Controls F.2 Physical Security Controls	11.1.1 Physical Security Perimeter 11.1.3 Securing Offices, Rooms, and Facilities 11.1.4 Protecting Against External and Environmental Threats 11.1.5 Working in Secure Areas 11.2.1 Equipment Sitting and Protection 11.2.3 Cabling Security 12.4.1 Event Logging
F.1.4.1	Do the physical security and environmental controls include restricted access and logs kept of all access?	Yes		Physical Security Program	Secure Workspace Access Reporting	F.2 Physical Security Controls F.5 Secure Workspace Access Reporting	11.1.1 Physical Security Perimeter 11.1.3 Securing Offices, Rooms, and Facilities 11.1.5 Working in Secure Areas 12.4.1 Event Logging 7.5.1 General
F.1.4.2	Do the physical security and environmental controls include electronic controlled access system (key card, token, fob, biometric reader, etc.)?	Yes		Physical Security Program	Secure Workspace Perimeter	F.2 Physical Security Controls F.4 Secure Workspace Perimeter	11.1.1 Physical Security Perimeter 11.1.5 Working in Secure Areas
F.1.4.3	Do the physical security and environmental controls include cipher locks (electronic or mechanical) to control access within or to the Facility?	Yes		Physical Security Program	Secure Workspace Perimeter	F.2 Physical Security Controls F.4 Secure Workspace Perimeter	11.1.1 Physical Security Perimeter
F.1.4.4	Do the physical security and environmental controls include security guards that provide onsite security services?	Yes		Physical Security Program	Secure Workspace Perimeter	F.2 Physical Security Controls F.4 Secure Workspace Perimeter	11.1.1 Physical Security Perimeter
F.1.4.5	Do the physical security and environmental controls include perimeter physical barrier (such as fence or walls)?	Yes		Physical Security Program	Secure Workspace Perimeter	F.2 Physical Security Controls	11.1.1 Physical Security Perimeter
F.1.4.6	Do the physical security and environmental controls include entry and exit doors alarmed (forced entry, propped open) and/or monitored by security guards?	Yes		Physical Security Program	Secure Workspace Perimeter	F.2 Physical Security Controls	11.1.1 Physical Security Perimeter

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
F.1.4.7	Do the physical security and environmental controls include a mechanism to prevent Tailgating/Piggybacking?	Yes		Physical Security Program	Secure Workspace Perimeter	F.2 Physical Security Controls F.4 Secure Workspace Perimeter	
F.1.4.10	Do the physical security and environmental controls include exterior doors with external hinge pins?	Yes		Physical Security Program	Secure Workspace Perimeter		11.1.1 Physical Security Perimeter
F.1.4.11	Do the physical security and environmental controls include windows with contact or break alarms on all windows?	Yes		Physical Security Program	Secure Workspace Perimeter	F.2 Physical Security Controls	11.1.1 Physical Security Perimeter
F.1.4.12	Do the physical security and environmental controls include digital CCTV with video stored at least 90 days?	Yes		Physical Security Program	Secure Workspace Perimeter	F.2 Physical Security Controls	
F.1.4.13	Do the physical security and environmental controls include fluid sensor?	Yes		Physical Security Program	Environmental Controls - Computer Hardware	F.1 Environmental Controls	11.1.4 Protecting Against External and Environmental Threats 11.2.1 Equipment Sitting and Protection
F.1.4.14	Do the physical security and environmental controls include HVAC and humidity controls?	Yes		Physical Security Program	Environmental Controls - Computer Hardware	F.1 Environmental Controls	11.1.4 Protecting Against External and Environmental Threats 11.2.1 Equipment Sitting and Protection
F.1.4.15	Do the physical security and environmental controls include heat detectors?	Yes		Physical Security Program	Environmental Controls - Computer Hardware	F.1 Environmental Controls	11.1.4 Protecting Against External and Environmental Threats 11.2.1 Equipment Sitting and Protection
F.1.4.16	Do the physical security and environmental controls include smoke detectors?	Yes		Physical Security Program	Environmental Controls - Computer Hardware	F.1 Environmental Controls	11.1.4 Protecting Against External and Environmental Threats 11.2.1 Equipment Sitting and Protection
F.1.4.17	Do the physical security and environmental controls include fire suppression?	Yes		Physical Security Program	Environmental Controls - Computer Hardware	F.1 Environmental Controls	11.1.4 Protecting Against External and Environmental Threats 11.2.1 Equipment Sitting and Protection
F.1.4.22	**Do physical access control procedures exist?**	Yes		Physical Security Program	Secure Workspace Access Reporting	H.7 Physical Access Controls	11.1.2 Physical Entry Controls 11.1.5 Working in Secure Areas 6.1.2 Segregation of Duties
F.1.4.22.1	Do physical access control procedures include segregation of duties for issuing and approving access?	Yes		Physical Security Program	Secure Workspace Access Reporting	H.7 Physical Access Controls	11.1.2 Physical Entry Controls 11.1.5 Working in Secure Areas 6.1.2 Segregation of Duties
F.1.4.22.2	Do physical access control procedures include access reviews at least every six months?	Yes		Physical Security Program	Secure Workspace Access Reporting	H.7 Physical Access Controls	11.1.2 Physical Entry Controls 11.1.5 Working in Secure Areas
F.1.4.22.3	Do physical access control procedures include collection of access equipment (badges, keys, change pin numbers, etc.) upon termination or status change?	Yes		Physical Security Program	Secure Workspace Access Reporting	H.2 Revoke System and Physical Access	11.1.2 Physical Entry Controls 11.1.5 Working in Secure Areas 9.2.6 Removal or Adjustment of Access Rights
F.1.4.22.4	Do physical access control procedures include lost or stolen access card/key reporting required?	Yes		Physical Security Program	Secure Workspace Access Reporting		11.1.2 Physical Entry Controls 11.1.5 Working in Secure Areas
F.2	**Are visitors permitted in the facility?**	No		Physical Security Program	Visitor Management	F.7 Visitor Management	11.1.2 Physical Entry Controls
F.2.1	Are visitors required to sign in and out?	N/A		Physical Security Program	Visitor Management	F.7 Visitor Management	11.1.2 Physical Entry Controls
F.2.2	Are visitors required to provide a government issued ID?	N/A		Physical Security Program	Visitor Management	F.7 Visitor Management	11.1.2 Physical Entry Controls
F.2.3	Are visitors required to be escorted through secure areas?	N/A		Physical Security Program	Visitor Management	F.7 Visitor Management	11.1.2 Physical Entry Controls
F.2.4	Are visitors required to wear badge distinguishing them from employees?	N/A		Physical Security Program	Visitor Management	F.7 Visitor Management	11.1.2 Physical Entry Controls

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
F.2.5	Are visitors logs maintained for at least 90 days?	N/A		Physical Security Program	Visitor Management	F.7 Visitor Management	11.1.2 Physical Entry Controls 12.4.1 Event Logging 7.5.1 General
F.3	Is there a loading dock at the facility?	Yes		Loading Dock Controls	Secure Workspace Perimeter		11.1.6 Delivery and Loading Areas
F.4	Is there a battery/UPS room in offices and/or facility?	Yes		Battery/UPS Room Controls	Physical Security Controls - Scoped Data	F.1 Environmental Controls	11.2.2 Supporting Utilities 12.4.1 Event Logging
F.5	Is there a generator or generator area in offices and/or facility?	Yes		Power Generator Controls	Physical Security Controls - Scoped Data	F.1 Environmental Controls	11.1.4 Protecting Against External and Environmental Threats 11.2.1 Equipment Sitting and Protection 11.2.2 Supporting Utilities 12.4.1 Event Logging
F.7	Is there a media library to store Scoped Data?	Yes		Media Library Controls	Physical Security Controls - Scoped Data		11.1.3 Securing Offices, Rooms, and Facilities 11.2.1 Equipment Sitting and Protection 12.4.1 Event Logging
F.8	Is there a telecom equipment room?	Yes		Telecom Equipment Room Controls	Physical Security Controls - Scoped Data		11.1.3 Securing Offices, Rooms, and Facilities 11.2.1 Equipment Sitting and Protection 11.2.3 Cabling Security 12.4.1 Event Logging
F.9	**Are your devices located in a locked server cabinet within the data center?**	Yes		Information Technology Device Physical Security	Physical Security Controls - Scoped Data	F.3 Secure Workspace Program	11.1.3 Securing Offices, Rooms, and Facilities 11.2.1 Equipment Sitting and Protection 12.4.1 Event Logging
F.9.1	Do server cabinets include restricted access and are logs kept of all access?	Yes		Information Technology Device Physical Security	Physical Security Controls - Scoped Data	F.4 Secure Workspace Perimeter	11.1.3 Securing Offices, Rooms, and Facilities 11.2.1 Equipment Sitting and Protection 12.4.1 Event Logging
F.9.2	Do server cabinets include Digital CCTV and video stored at least 90 days?	Yes		Information Technology Device Physical Security	Video Monitoring	F.4 Secure Workspace Perimeter	11.1.3 Securing Offices, Rooms, and Facilities 11.2.1 Equipment Sitting and Protection
F.10	**Do the Scoped Systems and Data reside in a data center?**	Yes		Data Center Controls	Physical Security Controls - Scoped Data		11.1.3 Securing Offices, Rooms, and Facilities
F.10.1	Do other tenants use the data center?	Yes		Data Center Controls	Secure Workspace Perimeter		11.1.3 Securing Offices, Rooms, and Facilities
F.10.2	Are locking screensavers on unattended system displays or locks on consoles required within the data center?	Yes		Data Center Controls	Physical Security Controls - Scoped Data	F.3 Secure Workspace Program F.6 Secure Workspace Compliance Inspections	11.1.3 Securing Offices, Rooms, and Facilities 11.1.5 Working in Secure Areas 11.2.1 Equipment Sitting and Protection 11.2.8 Unattended User Equipment 11.2.9 Clear Desk and Clear Screen Policy
F.10.3	Is there a procedure for equipment removal from the data center?	Yes		Data Center Controls	Physical Security Controls - Scoped Data	F.2 Physical Security Controls	11.2.1 Equipment Sitting and Protection 11.2.5 Removal of Assets 11.2.6 Security Equipment and Assets Off Premises

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
F.10.4	Are maintenance contracts maintained for critical equipment?	Yes		Data Center Controls	Maintenance Contracts for Critical Equipment		11.1.4 Protecting Against External and Environmental Threats 11.2.1 Equipment Sitting and Protection 11.2.2 Supporting Utilities 11.2.4 Equipment Maintenance
F.10.5	**Are tests conducted for any building systems?**	Yes		Data Center Controls	Physical and Environmental Security Testing	F.8 Physical and Environmental Security Testing	11.1.4 Protecting Against External and Environmental Threats
F.10.5.1	Are UPS systems tested at least annually?	Yes		Data Center Controls	Physical and Environmental Security Testing	F.8 Physical and Environmental Security Testing	11.1.4 Protecting Against External and Environmental Threats
F.10.5.2	Are all security alarm systems tested at least annually?	Yes		Data Center Controls	Physical and Environmental Security Testing	F.8 Physical and Environmental Security Testing	11.1.4 Protecting Against External and Environmental Threats
F.10.5.3	Are all fire alarms tested at least annually?	Yes		Data Center Controls	Physical and Environmental Security Testing	F.8 Physical and Environmental Security Testing	11.1.4 Protecting Against External and Environmental Threats
F.10.5.4	Are all fire suppression systems tested at least annually?	Yes		Data Center Controls	Physical and Environmental Security Testing	F.8 Physical and Environmental Security Testing	11.1.4 Protecting Against External and Environmental Threats
F.10.5.5	Are all generators tested at least monthly?	Yes		Data Center Controls	Physical and Environmental Security Testing	F.8 Physical and Environmental Security Testing	11.1.4 Protecting Against External and Environmental Threats
F.10.5.6	Are all generators full-load tested at least monthly?	Yes		Data Center Controls	Physical and Environmental Security Testing	F.8 Physical and Environmental Security Testing	11.1.4 Protecting Against External and Environmental Threats

G. Operations Management

Scoped As: SIG Core 2019 **Progress:** 100% **Tab Automation:** Enable

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 in column F to provide.
- To display the entire contents of the tab, select the word "Disable" in the Tab Automation field at the top of the page.
- Use the Maturity column to identify the Maturity of the question. See the How To Guide for instructions on filling out this field.

Note: There may be gaps in the question number sequence depending on how the issues/outsourcer generated the SIG.

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
G.1	**Are management approved operating procedures utilized?**	Yes		Operational Procedures and Responsibilities	IT Operational Procedures		12.1.1 Documented Operating Procedures
G.1.1	Are operating procedures documented, maintained, and made available to all users?	Yes		Operational Procedures and Responsibilities	IT Operational Procedures		12.1.1 Documented Operating Procedures
G.2	**Is there an operational change management/Change Control policy or program that has been documented, approved by management, communicated to appropriate Constituents and assigned an owner to maintain and review the policy?**	Yes		Operational Procedures and Responsibilities	Change Control	G.1 Change Control	12.1.2 Change Management 8.1 Operational Planning and Control
G.2.5	Does the operational change management/Change Control policy or program include communication of changes to all relevant Constituents?	Yes		Operational Procedures and Responsibilities	Change Control	G.1 Change Control	12.1.2 Change Management
G.2.10	**Do changes to the production environment including network, systems, application updates, and code changes subject to the change control process?**	Yes		Operational Procedures and Responsibilities	Change Control	G.1 Change Control	12.1.2 Change Management
G.2.10.1	Does the change control process include segregation of duties between those requesting, approving and implementing a change?	Yes		Operational Procedures and Responsibilities	Change Control	G.1 Change Control	12.1.2 Change Management 6.1.2 Segregation of Duties
G.2.10.2	Does the change control process include a formal process to ensure clients are notified prior to changes being made which may impact their service?	Yes		Operational Procedures and Responsibilities	Change Control	G.1 Change Control	12.1.2 Change Management 12.7.1 Information Systems Audit Controls
G.2.10.3	**Does the change control process include a scheduled maintenance window?**	Yes		Operational Procedures and Responsibilities	Change Control		12.1.2 Change Management 12.7.1 Information Systems Audit Controls
G.2.10.3.1	Does the change control process include a scheduled maintenance window which results in client downtime?	Yes		Operational Procedures and Responsibilities	Change Control		12.1.2 Change Management 12.7.1 Information Systems Audit Controls
G.2.10.5	Does the change control process include an option for clients to opt-in or opt-out of specific features in releases?	Yes		Operational Procedures and Responsibilities	Change Control		
G.2.10.6	Does the change control process require evidence that Information security activities will not adversely affect existing systems, particularly at peak processing times, such as month end?	Yes		Operational Procedures and Responsibilities	Change Control	G.1 Change Control	12.1.3 Capacity Management
G.3	**Are Information security requirements specified and implemented when new systems are introduced, upgraded, or enhanced?**	Yes		Operational Procedures and Responsibilities	System Acceptance Criteria	B.2 Information Security Standards G.1 Change Control	12.1.3 Capacity Management 12.6.1 Management of Technical Vulnerabilities 14.1.1 Information Security Requirements Analysis and Specification
G.3.1	Are new, upgraded or enhanced systems required to include a determination of security requirements based on the sensitivity of the data?	Yes		Operational Procedures and Responsibilities	System Acceptance Criteria	B.2 Information Security Standards G.1 Change Control	14.1.1 Information Security Requirements Analysis and Specification
G.3.2	Are Information security specifications for new, upgraded or enhanced systems identified using requirements from policies and regulations, threat modeling, incident reviews, or use of vulnerability thresholds?	Yes		Operational Procedures and Responsibilities	System Acceptance Criteria	B.2 Information Security Standards G.1 Change Control	12.6.1 Management of Technical Vulnerabilities 14.1.1 Information Security Requirements Analysis and Specification
G.3.3	Are security specifications implemented prior to the introduction of a new information system, upgrade, or enhancement to the environment?	Yes		Operational Procedures and Responsibilities	System Acceptance Criteria	B.2 Information Security Standards G.1 Change Control	14.1.1 Information Security Requirements Analysis and Specification

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
G.3.4	Are controls and associated processes related to security specifications such as authentication, access control, provisioning, and training considered for new, upgraded or enhanced systems?	Yes		Operational Procedures and Responsibilities	System Acceptance Criteria	B.2 Information Security Standards G.1 Change Control	14.1.1 Information Security Requirements Analysis and Specification
G.3.6	Are business continuity requirements considered for new, upgraded or enhanced systems?	Yes		Operational Procedures and Responsibilities	System Acceptance Criteria	G.1 Change Control K.1 Business Resiliency Governance	12.1.3 Capacity Management
G.3.7	Are performance and computer capacity requirements considered for new, upgraded or enhanced systems?	Yes		Operational Procedures and Responsibilities	System Acceptance Criteria	G.1 Change Control	12.1.3 Capacity Management
G.4	Do systems and network devices utilize a common time synchronization service?	Yes		Operational Procedures and Responsibilities	Time Synchronization	J.6 IS/IT Incident Management – Analysis	12.4.4 Clock Synchronization

H. Access Control

Scoped As: SIG Core 2019 **Progress:** 100% **Tab Automation:** Enable

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 in column F to provide.
- To display the entire contents of the tab, select the word "Disable" in the Tab Automation field at the top of the page.
- Use the Maturity column to identify the Maturity of the question. See the How To Guide for instructions on filling out this field.

Note: There may be gaps in the question number sequence depending on how the issues/outsourcer generated the SIG.

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
H.1	**Are electronic systems used to transmit, process or store Scoped Systems and Data?**	Yes		Access Control	Scoping		
H.1.1	Is there an access control program that has been approved by management, communicated to Constituents and an owner to maintain and review the program?	Yes		Access Control	Policy		9.1.1 Access Control Policy 9.2.1 User Registration and De-registration 9.4.1 Information Access Restriction
H.2	Are Constituents able to access Scoped Data?	Yes		Access Control	Operations Staff Access	H.3 Logical Access Authorization	
H.3	Can clients receive a list of personnel who have access to their Scoped Systems and Data?	No		Access Control	Operations Staff Access		
H.4	Is the use of system utilities restricted to authorized users only?	Yes		Access Control	System Utility Access Control	H.8 Restrictions and Multifactor Authentication for Remote Access	9.4.4 Use of Privilege Utility Programs
H.5	**Are unique individual IDs required for user authentication to applications, operating systems, databases and network devices?**	Yes		Access Provisioning	Identity Management	H.1 Password Controls	9.2.1 User Registration and De-registration 9.4.1 Information Access Restriction 9.4.2 Secure Log-on Procedure
H.5.1	**Are user IDs created with naming conventions that either identifies roles or Access levels, or contain personal information other than name (i.e. SSN, Access Level, Admin role)?**	Yes		Access Provisioning	Identity Management	H.1 Password Controls	9.2.1 User Registration and De-registration
H.5.1.1	Are standards based federated ID capability available to clients (e.g., SAML, OpenID, Single Sign On)?	Yes		Access Provisioning	Federated Identity Management		6.2.2 Teleworking
H.6	Is there an internet-accessible Self-Service portal available that allows clients to provision, audit, modify, and remove user entitlements?	No		Access Provisioning	Self-Service Portal	V.3 Cloud Audit Program	
H.7	Is access on applications, operating systems, databases, and network devices provisioned according to the principle of least privilege?	Yes		Access Provisioning	Access Least Privilege	H.3 Logical Access Authorization	9.1.1 Access Control Policy 9.1.2 Access to Networks and Network Services 9.2.1 User Registration and De-registration 9.4.1 Information Access Restriction
H.8	**Is there a process to request and receive approval for access to systems transmitting, processing or storing Scoped Systems and Data?**	Yes		Access Provisioning	Access Approval	H.3 Logical Access Authorization	6.1.2 Segregation of Duties 9.2.2 User Access Provisioning
H.8.1	**Is there segregation of duties for granting access and approving access to Scoped Systems and Data?**	Yes		Access Provisioning	Access Approval	H.3 Logical Access Authorization	6.1.2 Segregation of Duties 9.2.2 User Access Provisioning
H.8.1.1	Is there segregation of duties for approving and implementing access requests for Scoped Systems and Data?	Yes		Access Provisioning	Access Approval	H.3 Logical Access Authorization	11.1.5 Working in Secure Areas 6.1.2 Segregation of Duties 9.2.2 User Access Provisioning
H.8.1.2	Where segregation of duties is not feasible, are activity monitoring, audit trail, and/or management supervision controls in place?	Yes		Access Provisioning	Access Approval	H.3 Logical Access Authorization	11.1.5 Working in Secure Areas 6.1.2 Segregation of Duties 9.2.2 User Access Provisioning
H.8.2	Are requests for granting access documented, retained and retrievable for audit purposes for a minimum of a year?	Yes		Access Provisioning	Access Approval	H.3 Logical Access Authorization	9.1.1 Access Control Policy 9.2.2 User Access Provisioning
H.8.3	Is access to systems that store or process scoped data limited?	Yes		Authentication	Access Restrictions		9.4.1 Information Access Restriction
H.8.6	**Is Multi-factor Authentication deployed?**	Yes		Authentication	Multi-Factor Authentication	H.8 Restrictions and Multifactor Authentication for Remote Access	9.2.3 Management of Privileged Access Rights 9.4.2 Secure Log-on Procedure

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
H.8.6.1	Is Multi-factor Authentication required for VPN?	Yes		Authentication	Multi-Factor Authentication		
H.8.6.2	Is Multi-factor Authentication required for Privileged System Access?	Yes		Authentication	Multi-Factor Authentication	H.8 Restrictions and Multifactor Authentication for Remote Access	9.2.3 Management of Privileged Access Rights 9.4.2 Secure Log-on Procedure
H.8.6.3	Is Multi-factor Authentication required for Scoped Systems and Data Access?	Yes		Authentication	Multi-Factor Authentication	H.8 Restrictions and Multifactor Authentication for Remote Access	9.4.2 Secure Log-on Procedure
H.8.6.4	Does system policy require terminating or securing active sessions when finished?	Yes		Inactivity Controls	Session Locking Requirement	H.5 Controls for Unattended Systems	11.1.5 Working in Secure Areas 11.2.8 Unattended User Equipment 9.3.1 Use of Secret Authentication Information 9.4.2 Secure Log-on Procedure
H.8.6.5	Does system policy require logoff from terminals, PC or servers when the session is finished?	Yes		Inactivity Controls	Account Logoff Requirement	H.5 Controls for Unattended Systems	11.1.5 Working in Secure Areas 11.2.8 Unattended User Equipment 9.3.1 Use of Secret Authentication Information 9.4.2 Secure Log-on Procedure
H.8.7	**Are user access rights reviewed periodically?**	Yes		Access Reviews	Entitlement Reviews	H.9 Monitoring of System Access Rights	9.1.1 Access Control Policy 9.2.5 Review of User Access Rights
H.8.7.1	Are user access rights reviewed at least quarterly?	No	Bi-monthly	Access Reviews	Entitlement Reviews	H.9 Monitoring of System Access Rights	9.1.1 Access Control Policy 9.2.5 Review of User Access Rights
H.8.8	Are access rights reviewed when a constituent changes roles?	Yes		Access Reviews	Entitlement Reviews	H.9 Monitoring of System Access Rights	9.1.1 Access Control Policy 9.2.5 Review of User Access Rights 9.2.6 Removal or Adjustment of Access Rights
H.8.9	**Are privileged user access rights reviewed periodically?**	Yes		Access Reviews	Privileged User Access Reviews	H.6 Privileged Accounts	9.1.1 Access Control Policy 9.2.3 Management of Privileged Access Rights 9.2.5 Review of User Access Rights
H.8.9.1	Are privileged user access rights reviewed at least quarterly?	Yes		Access Reviews	Privileged User Access Reviews	H.6 Privileged Accounts	9.1.1 Access Control Policy 9.2.3 Management of Privileged Access Rights 9.2.5 Review of User Access Rights
H.8.10	Are changes to privileged user access rights logged?	Yes		Access Reviews	Privileged User Access Reviews	H.6 Privileged Accounts	12.4.1 Event Logging 9.1.1 Access Control Policy 9.2.3 Management of Privileged Access Rights 9.2.5 Review of User Access Rights
H.8.11	Is the Service Provider responsible for performing all user entitlement audits of Service Provider personnel and subcontractors with access to Scoped Systems and Data? If no, please explain.	Yes		Access Reviews	Entitlement Reviews	G.3 Application Security Vulnerability Assessment and Remediation	
H.8.12	Is an inactive user ID disabled within 90 days?	Yes		Access Revocation	Inactive User Access Revocation	H.4 Inactive Accounts	9.2.1 User Registration and De-registration
H.8.13	Is an inactive user ID deleted within 120 days?	Yes		Access Revocation	Inactive User Access Revocation	H.4 Inactive Accounts	9.2.1 User Registration and De-registration
H.9	**Are passwords used?**	Yes		Password Controls	Scoping	H.1 Password Controls	

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
H.9.1	**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 and network devices? If no, please explain in the 'Additional Information' field.**	Yes		Password Controls	Password Policy	H.1 Password Controls	11.1.5 Working in Secure Areas 11.2.8 Unattended User Equipment 9.2.4 Management of Secret Authentication Information of Users 9.3.1 Use of Secret Authentication Information 9.4.2 Secure Log-on Procedure 9.4.3 Password Management System
H.9.1.5	Does password policy include minimum password length at least eight characters?	Yes		Password Controls	Minimum Password Length	H.1 Password Controls	9.3.1 Use of Secret Authentication Information 9.4.3 Password Management System
H.9.1.6	Are complex passwords (mix of upper case letters, lower case letters, numbers, and special characters) required on systems transmitting, processing, or storing Scoped Data?	Yes		Password Controls	Password Complexity	H.1 Password Controls	9.2.4 Management of Secret Authentication Information of Users 9.3.1 Use of Secret Authentication Information 9.4.2 Secure Log-on Procedure 9.4.3 Password Management System
H.9.1.8	Does password policy require initial and temporary passwords to be changed upon next login?	Yes		Password Controls	Initial Password Requirements	H.1 Password Controls	9.2.4 Management of Secret Authentication Information of Users 9.3.1 Use of Secret Authentication Information 9.4.3 Password Management System
H.9.1.9	Does password policy require initial and temporary passwords to be random and complex?	Yes		Password Controls	Initial Password Requirements	H.1 Password Controls	9.2.4 Management of Secret Authentication Information of Users 9.3.1 Use of Secret Authentication Information 9.4.3 Password Management System
H.9.1.10	Does password policy prohibit users from sharing passwords?	Yes		Password Controls	Password sharing prohibition	H.1 Password Controls	9.2.4 Management of Secret Authentication Information of Users 9.3.1 Use of Secret Authentication Information
H.9.1.11	Does password policy require keeping passwords confidential?	Yes		Password Controls	Password confidentiality	H.1 Password Controls	9.2.4 Management of Secret Authentication Information of Users 9.3.1 Use of Secret Authentication Information
H.9.1.12	Does password policy prohibit keeping an unencrypted record of passwords (paper, software file or handheld device)?	Yes		Password Controls	Unencrypted password prohibition		9.2.4 Management of Secret Authentication Information of Users 9.3.1 Use of Secret Authentication Information
H.9.1.13	Does password policy require changing passwords when there is an indication of possible system or password compromise?	Yes		Password Controls	Password change upon potential compromise	H.1 Password Controls	9.2.4 Management of Secret Authentication Information of Users 9.3.1 Use of Secret Authentication Information 9.4.3 Password Management System

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
H.9.1.14	Does password policy require changing passwords at regular intervals?	Yes		Password Controls	Regular password change	H.1 Password Controls	9.3.1 Use of Secret Authentication Information 9.4.3 Password Management System
H.9.1.15	Does password policy require password expiration within 90 days or less?	Yes		Password Controls	Password Expiration	H.1 Password Controls	9.3.1 Use of Secret Authentication Information 9.4.3 Password Management System
H.9.1.17	Does password policy prohibit including unencrypted passwords in automated logon processes (e.g., stored in a macro or function key)?	Yes		Password Controls	Automated logon password storage prohibition	H.1 Password Controls U.1 System Configuration and Hardening Standards	9.4.2 Secure Log-on Procedure 9.4.3 Password Management System
H.9.1.18	Does password policy prohibit a PIN or secret question as a possible stand-alone method of authentication?	Yes		Password Controls	Password Complexity	U.1 System Configuration and Hardening Standards	9.4.2 Secure Log-on Procedure
H.9.2	Does password policy require passwords to be encrypted in transit?	Yes		Password Controls	Password Cryptography	U.1 System Configuration and Hardening Standards	
H.9.3	**Does password policy require passwords to be encrypted or hashed in storage?**	Yes		Password Controls	Password Cryptography	U.1 System Configuration and Hardening Standards	
H.9.3.1	Does password policy require passwords to be hashed using a Key Derivation Function (PBKDF2, Script, Bcrypt)?	Yes		Password Controls	Password Cryptography		
H.9.4	Does password policy require that passwords are masked when entered and displayed?	Yes		Password Controls	Password Cryptography	H.1 Password Controls	
H.9.5	Does password policy require system configuration to lock an account when five or more invalid login attempts are made?	Yes		Password Controls	Password Lockout	H.1 Password Controls	9.4.2 Secure Log-on Procedure
H.9.7	Is password reset authority restricted to authorized persons and/or an automated password reset tool?	Yes		Password Controls	Password Reset	H.1 Password Controls	
H.9.8	Are password files and application data stored in different file systems?	Yes		Password Controls	Password and Application Data Segregation	H.1 Password Controls	
H.9.9	Are user IDs and passwords communicated/distributed via separate media (e.g., e-mail and phone)?	Yes		Password Controls	User IDs and Password Channel Segregation	H.8 Restrictions and Multifactor Authentication for Remote Access	
H.10	**Is Remote Access permitted?**	Yes		Remote Access	Scoping	H.8 Restrictions and Multifactor Authentication for Remote Access	6.2.2 Teleworking
H.10.1	Are encrypted communications required for all remote connections?	Yes		Remote Access	Encryption	H.8 Restrictions and Multifactor Authentication for Remote Access	6.2.2 Teleworking
H.10.2	**Is multi-factor authentication required for remote access?**	Yes		Remote Access	Multi-Factor Authentication	H.8 Restrictions and Multifactor Authentication for Remote Access	6.2.2 Teleworking
H.10.2.1	Is multi-factor authentication required to remotely access the production environment containing Scoped Data?	Yes		Remote Access	Multi-Factor Authentication	U.1 System Configuration and Hardening Standards	6.2.2 Teleworking
H.10.2.4	Is multi-factor authentication required for remote admin local system access (shell or UI)?	Yes		Remote Access	Multi-Factor Authentication	H.3 Logical Access Authorization H.8 Restrictions and Multifactor Authentication for Remote Access	6.2.2 Teleworking

I. Application Security

Scoped As: SIG Core 2019 **Progress:** 100% **Tab Automation:** Enable

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 in column F to provide.
- To display the entire contents of the tab, select the word "Disable" in the Tab Automation field at the top of the page.
- Use the Maturity column to identify the Maturity of the question. See the How To Guide for instructions on filling out this field.

Note: There may be gaps in the question number sequence depending on how the issues/outsourcer generated the SIG.

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
I.1	**Are applications used to transmit, process or store Scoped Data?**	Yes		Application Security	Scoping		14.1.2 Securing Application Services on Public Networks 14.1.3 Protecting Application Services Transactions
I.1.1	Is there an individual or group responsible for Application Security?	Yes		Application Security Roles and Responsibilities	Application Security Responsibility	I.1 Application Security Program Governance	
I.1.2	**Is there formal software security training for developers?**	Yes		Application Security Roles and Responsibilities	Developer Training	I.20 Application Security Awareness Training Attendance and Certification	
I.1.2.1	Do application security experts work with developers for every application?	Yes		Application Security Roles and Responsibilities	Secure DevOps		
I.1.2.2	**Are outside development resources utilized?**	No		Application Security Roles and Responsibilities	External Developers		14.2.7 Outsourced Development
I.1.2.2.1	Do all outside development resources comply with the SDLC (Software Development Life Cycle)?	N/A	Outsourced developers are not used.	Application Security Roles and Responsibilities	External Developers		14.2.7 Outsourced Development
I.1.3	**Do changes to applications or application code go through a risk assessment?**	Yes		Secure Architectural Design Standards	New Platform Secure Architecture Risk Analysis	I.1 Application Security Program Governance	
I.1.3.1	Is a security architecture risk analysis performed when new applications are designed?	Yes		Secure Architectural Design Standards	New Platform Secure Architecture Risk Analysis	I.8 Secure Architectural Design Standards	
I.1.3.6	Do security architecture risk analyses assign applications risk ratings that reflect the types of data accessed (e.g., high, medium, low)?	Yes		Secure Architectural Design Standards	New Platform Secure Architecture Risk Analysis	I.6 Risk Classification	
I.1.4	Are the risks from internal and external sources clearly understood based on risk exposure?	Yes		Secure Architectural Design Standards	New Platform Secure Architecture Risk Analysis	I.6 Risk Classification	
I.1.6	Is a formal application methodology used (e.g., Agile, DSDM, XP, FDD, LD)? If yes, please list in Additional Information.	Yes	Agile	Secure Architectural Design Standards	Design Methodology	I.4 Secure Systems Development Life Cycle (SDLC) Code Reviews	
I.1.7	Is every data transaction maintained in an authenticated state?	Yes		Secure Architectural Design Standards	State Management	I.2 Secure Systems Development Life Cycle (SDLC) Policies, Standards and Procedures	14.1.2 Securing Application Services on Public Networks 14.1.3 Protecting Application Services Transactions
I.1.8	Is there a means for secure session management?	Yes		Secure Architectural Design Standards	Session Management	I.2 Secure Systems Development Life Cycle (SDLC) Policies, Standards and Procedures	14.1.2 Securing Application Services on Public Networks 14.1.3 Protecting Application Services Transactions
I.1.9	Is there comprehensive, secure error handling?	Yes		Secure Architectural Design Standards	Secure Error Handling	I.2 Secure Systems Development Life Cycle (SDLC) Policies, Standards and Procedures	14.1.3 Protecting Application Services Transactions
I.1.10	Do audit log failures generate an alert?	Yes		Secure Architectural Design Standards	Application Logging	U.1 System Configuration and Hardening Standards	
I.1.11	Do applications provide granular and comprehensive logging?	Yes		Secure Architectural Design Standards	Application Logging		12.4.1 Event Logging
I.1.13	Are system, vendor, or service accounts disallowed for normal operations and monitored for usage?	Yes		Secure Architectural Design Standards	Service Account Management		

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
I.1.14	Are web applications configured to follow best practices or security guidelines (e.g., OWASP)?	Yes		Secure Architectural Design Standards	Web Security Standards		
I.1.15	Is data input into applications validated?	Yes		Secure Architectural Design Standards	Application Data Integrity		14.1.3 Protecting Application Services Transactions
I.1.16	Are development, test, and staging environment separate from the production environment?	Yes		Secure Architectural Design Standards	Application Environment Segmentation	G.1 Change Control	12.1.4 Separation of Development, Testing, and Operational Environments 14.2.6 Secure Development Environments
I.1.17	Do applications have separate source code repositories for production and non-production environments?	Yes		Secure Architectural Design Standards	Application Environment Segmentation	I.2 Secure Systems Development Life Cycle (SDLC) Policies, Standards and Procedures	9.4.5 Access Control to Program Source Code
I.1.18	Do IT support personnel have access to application source libraries?	No		Secure Architectural Design Standards	Application Source Library Access Control	I.14 Web Server and Application Log on Activity Logging	9.4.5 Access Control to Program Source Code
I.1.19	**Is all access to application source libraries logged?**	Yes		Secure Architectural Design Standards	Application Source Library Access Control		12.4.1 Event Logging 9.4.5 Access Control to Program Source Code
I.1.19.1	Are audit logs maintained and reviewed for all application source library updates?	Yes		Secure Architectural Design Standards	Application Source Library Access Control	I.1 Application Security Program Governance	12.4.1 Event Logging 9.4.5 Access Control to Program Source Code
I.1.20	**Are developers permitted to access production environments, including read only access?**	No		Secure Architectural Design Standards	Developer Access Control		
I.1.20.2	Are developers required to request or obtain access outside an established role (emergency access)?	N/A	Not allowed access	Secure Architectural Design Standards	Developer Access Control		
I.1.21	**Are Scoped Systems and Data used in the test, development, or QA environments?**	No		Secure Architectural Design Standards	Test Data Access Control	I.13 Protection of Scoped Data in a Non-Production Environment	14.3.1 Protection of Test Data
I.1.21.1	Is authorization required when production data is copied to the test environment?	N/A	Not used in production	Secure Architectural Design Standards	Test Data Access Control	I.13 Protection of Scoped Data in a Non-Production Environment	14.3.1 Protection of Test Data
I.1.21.2	Is test data destroyed following the testing phase?	Yes		Secure Architectural Design Standards	Test Data Access Control	I.13 Protection of Scoped Data in a Non-Production Environment	14.3.1 Protection of Test Data
I.1.21.3	Is test data masked or obfuscated during the testing phase?	Yes		Secure Architectural Design Standards	Test Data Access Control	I.13 Protection of Scoped Data in a Non-Production Environment	14.3.1 Protection of Test Data
I.2	**Is application development performed?**	Yes		SDLC	Scoping	I.1 Application Security Program Governance	
I.2.1	**Is there a formal Software Development Life Cycle (SDLC) process?**	Yes		SDLC	SDLC	I.2 Secure Systems Development Life Cycle (SDLC) Policies, Standards and Procedures	
I.2.1.1	Does the SDLC process include integration testing, and acceptance testing?	Yes		SDLC	SDLC	I.2 Secure Systems Development Life Cycle (SDLC) Policies, Standards and Procedures	
I.2.2	Is there a secure software development lifecycle policy that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?	Yes		SDLC	SDLC	I.2 Secure Systems Development Life Cycle (SDLC) Policies, Standards and Procedures	14.2.1 Secure Development Policy 14.2.5 Secure System Engineering Principles
I.2.3	**Is there a documented change management/change control process for applications with Scoped Data?**	Yes		SDLC	Application Change Control	G.1 Change Control I.2 Secure Systems Development Life Cycle (SDLC) Policies, Standards and Procedures	14.2.2 System Change Control Procedures 14.2.3 Technical Review of Applications After Operating Platform Changes 14.2.4 Restrictions on Changes to Software Packages 14.2.9 System Acceptance Testing

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
I.2.3.1	Are applications released to production on a fixed schedule? Identify the schedule (e.g., Daily, Weekly, Monthly, Ad-hoc) in the Additional Information field:	Yes	Ad-hoc	SDLC	Application Change Control	I.2 Secure Systems Development Life Cycle (SDLC) Policies, Standards and Procedures	
I.2.3.2	Does the application change management/change control process include change control procedures required for all changes to the production environment?	Yes		SDLC	Application Change Control	G.1 Change Control	12.4.1 Event Logging 14.2.2 System Change Control Procedures 14.2.3 Technical Review of Applications After Operating Platform Changes
I.2.3.3	Does the application change management/change control process include testing prior to deployment?	Yes		SDLC	Application Change Control	I.3 Application Security SDLC Phases I.10 Security Review of Externally Developed Applications	14.2.2 System Change Control Procedures 14.2.3 Technical Review of Applications After Operating Platform Changes 14.2.9 System Acceptance Testing
I.2.3.4	Does the application change management/change control process include management approval prior to deployment?	Yes		SDLC	Application Change Control	I.3 Application Security SDLC Phases I.10 Security Review of Externally Developed Applications	14.2.2 System Change Control Procedures 14.2.9 System Acceptance Testing
I.2.3.8	Does the application change management/change control process include stakeholder communication and/or approvals?	Yes		SDLC	Application Change Control	G.1 Change Control	14.2.2 System Change Control Procedures
I.2.3.9	Does the application change management/change control process include a list of individuals authorized to approve changes?	Yes		SDLC	Application Change Control	G.1 Change Control	14.2.2 System Change Control Procedures
I.2.3.10	Does the application change management/change control process include an impact assessment to review all affected systems and applications?	Yes		SDLC	Application Change Control	G.3 Application Security Vulnerability Assessment and Remediation I.7 Privacy Impact Analysis	14.2.2 System Change Control Procedures 14.2.3 Technical Review of Applications After Operating Platform Changes
I.2.3.11	Does the application change management/change control process include documentation for all system changes?	Yes		SDLC	Application Change Control	G.1 Change Control I.2 Secure Systems Development Life Cycle (SDLC) Policies, Standards and Procedures	14.2.2 System Change Control Procedures 14.2.3 Technical Review of Applications After Operating Platform Changes
I.2.3.12	Does the application change management/change control process include version control for all software?	Yes		SDLC	Application Change Control	I.1 Application Security Program Governance	14.2.2 System Change Control Procedures 14.2.3 Technical Review of Applications After Operating Platform Changes
I.2.3.13	Does the application change management/change control process include logging of all Change Requests?	Yes		SDLC	Application Change Control	G.1 Change Control	12.4.1 Event Logging 14.2.2 System Change Control Procedures
I.2.3.14	Does the application change management/change control process include changes only take place during specified and agreed upon times (green zone)?	Yes		SDLC	Application Change Control	G.1 Change Control	14.2.2 System Change Control Procedures
I.2.3.15	Does the application change management/change control process include modifications and changes to software are strictly controlled?	Yes		SDLC	Application Change Control	G.1 Change Control	14.2.2 System Change Control Procedures 14.2.3 Technical Review of Applications After Operating Platform Changes 14.2.4 Restrictions on Changes to Software Packages
I.2.4	**Are applications evaluated from a security perspective prior to promotion to production?**	Yes		SDLC	Application Security QA_UAT Process	I.12 QA_UAT Process	14.2.3 Technical Review of Applications After Operating Platform Changes 14.2.8 System Security Testing

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
I.2.4.1	Do pre-production application security reviews include testing procedures to determine whether security features are effective?	Yes		SDLC	Application Security QA_UAT Process	I.12 QA_UAT Process	14.2.3 Technical Review of Applications After Operating Platform Changes 14.2.8 System Security Testing
I.2.5	**Is code obtained from external sources reviewed for security flaws and backdoors prior to use in production?**	Yes		SDLC	Reviews of Code Obtained from External Sources	I.10 Security Review of Externally Developed Applications	
I.2.5.1	Is code obtained from external sources identified in application documentation as external code?	Yes		SDLC	Reviews of Code Obtained from External Sources		
I.2.5.2	Is code obtained from external sources reviewed for new versions at least every 6 months?	Yes		SDLC	Reviews of Code Obtained from External Sources		
I.2.5.3	**Is any code obtained from external sources open source?**	Yes		SDLC	Open Source Software Security	I.11 Open Source	
I.2.5.3.1	**Is open source software or libraries used to transmit, process or store Scoped Data?**	Yes		SDLC	Open Source Software Security	I.11 Open Source	
I.2.5.3.1.1	Are information security reviews conducted and approved for the use or installation of open source software (e.g., Linux, Apache, etc.)?	Yes		SDLC	Open Source Software Security	I.11 Open Source	
I.2.6	**Is a Secure Code Review performed regularly?**	Yes		SDLC	Secure Code Review	I.2 Secure Systems Development Life Cycle (SDLC) Policies, Standards and Procedures I.9 Secure Code Review	
I.2.6.1	Is there a full secure code review for each release? If no, please explain the secure code review schedule and scope in the 'Additional Information' field.	No	Source code is reviewed at least quarterly.	SDLC	Secure Code Review	I.9 Secure Code Review	
I.2.6.2	Are secure code reviews performed against the entire code base in the development phase? If not, please explain in the 'Additional Information' field.	No	Source code is reviewed at least quarterly.	SDLC	Secure Code Review	I.9 Secure Code Review	
I.2.6.3	Do secure code reviews include validation checks for the most critical web application security flaws including Cross Site Scripting, SQL injection (e.g., OWASP Top 10 vulnerabilities)?	Yes		SDLC	Secure Code Review	I.12 QA_UAT Process	
I.2.6.4	Do secure code reviews include regular analysis of vulnerability to recent attacks?	Yes		SDLC	Secure Code Review	I.12 QA_UAT Process	
I.2.6.6	Do secure code reviews include dynamic scanning against web based applications while in the Q/A phase?	Yes		SDLC	Secure Code Review	I.12 QA_UAT Process	
I.2.6.7	Do secure code reviews include testing against common code vulnerabilities?	Yes		SDLC	Secure Code Review	I.9 Secure Code Review	
I.2.6.8	Are secure code reviews performed by individuals qualified to identify and correct code security flaws?	Yes		SDLC	Secure Code Review	I.9 Secure Code Review	
I.2.6.9	Is source code security reviewed manually? If yes, identify the frequency (e.g., Daily, Weekly, Monthly, Ad-Hoc) in the additional information field.	No		SDLC	Secure Code Review	I.9 Secure Code Review	
I.2.6.10	Is an automated secure source code review conducted?	Yes		SDLC	Secure Code Review	I.9 Secure Code Review	
I.2.7	**Are identified security vulnerabilities remediated prior to promotion to production?**	Yes		SDLC	Vulnerability Remediation	I.12 QA_UAT Process	
I.2.7.1	Does the SDLC process include Remediation of Penetration Test issues relevant to the application under review?	Yes		SDLC	Vulnerability Remediation	I.12 QA_UAT Process	
I.2.7.2	Does the SDLC process include communicating discovered vulnerabilities to developers?	Yes		SDLC	Vulnerability Remediation	I.12 QA_UAT Process	
I.2.7.3	Does the SDLC process include communicating known un-remediated vulnerabilities to the Security Monitoring and Response group for awareness and monitoring?	Yes		SDLC	Vulnerability Remediation	I.12 QA_UAT Process	
I.3	**Is a web site supported, hosted or maintained that has access to Scoped Systems and Data?**	Yes		Web Server Security	Scoping		
I.3.1	Do you have logical or Physical segregation between web, application and database components? i.e., Internet, DMZ, Database?	No	Logical segmentation through firewall for portal service.	Web Server Security	Configuration Management	G.4 Website Setup, Operation and Security	13.1.3 Segregation in Networks
I.3.2	**Are Web Servers used for transmitting, processing or storing Scoped Data?**	Yes	Portal application only.	Web Server Security	Scoping		
I.3.2.1	Are security configuration standards documented for web server software?	Yes		Web Server Security	Web Server Security Standards	G.4 Website Setup, Operation and Security	

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
I.3.2.2	Are web server software security configuration standards reviewed and/or updated at least annually to account for any changes in environment, available security features and/or leading practices?	Yes		Web Server Security	Web Server Security Standards		
I.3.2.3	Are reviews performed to validate compliance with documented web server software security standards?	Yes		Web Server Security	Web Server Security Standards	G.4 Website Setup, Operation and Security	
I.3.2.4	**Is HTTPS enabled for all web pages?**	Yes		Web Server Security	Web Encryption Security	D.6 Network Management – Encrypted Authentication Credentials	
I.3.2.4.1	Are either TLS 1.2 or 1.3 used for Encrypting all web pages used?	Yes		Web Server Security	Web Encryption Security		
I.3.2.4.2	Are web server certificates centrally managed and kept current?	Yes		Web Server Security	Web Encryption Security	G.4 Website Setup, Operation and Security	
I.3.2.5	Are all unnecessary/unused services in web server software uninstalled or disabled?	Yes		Web Server Security	Administrative and File Sharing Service Security	G.4 Website Setup, Operation and Security	
I.3.2.7	Are all remote administration and file sharing services on web server software configured to require authentication and encryption?	Yes		Web Server Security	Administrative and File Sharing Service Security	G.4 Website Setup, Operation and Security H.8 Restrictions and Multifactor Authentication for Remote Access	
I.3.2.9	Are sample applications and scripts removed from web servers?	Yes		Web Server Security	Web Server Hardening		
I.3.2.10	Are all web server software files maintained separate from the Operating System?	Yes		Web Server Security	Web Server Hardening	N.2 Network Security – Firewall(s) and/or Other Devices Providing the Same Functionality U.1 System Configuration and Hardening Standards	
I.3.2.11	Are available high-risk web server software security patches applied and verified at least monthly?	Yes		Web Server Security	Web Server Vulnerability Management	G.2 System Patching	14.2.9 System Acceptance Testing
I.3.2.12	**Are all web server software patching exceptions documented and approved by information security or senior management?**	Yes		Web Server Security	Web Server Vulnerability Management	G.2 System Patching	14.2.9 System Acceptance Testing
I.3.2.12.1	Are web server software patches, service packs, and hot fixes tested prior to installation?	Yes		Web Server Security	Web Server Vulnerability Management	G.2 System Patching	14.2.9 System Acceptance Testing
I.3.2.12.4	Are third party alert services used to keep up to date with the latest web server software vulnerabilities?	Yes		Web Server Security	Web Server Vulnerability Management	U.1 System Configuration and Hardening Standards	
I.3.2.12.5	Are web server software versions that no longer have security patches released prohibited?	Yes		Web Server Security	Web Server Vulnerability Management	U.1 System Configuration and Hardening Standards	
I.3.2.13	Are web server software configuration options restricted to authorized users?	Yes		Web Server Security	Web Server Configuration Management	U.1 System Configuration and Hardening Standards	
I.3.2.14	**Is sufficient detail contained in Web Server and application logs to support incident investigation, including successful and failed login attempts and changes to sensitive configuration settings and files?**	Yes		Web Server Security	Web Server Auditing and Logging	J.6 IS/IT Incident Management – Analysis	
I.3.2.14.1	Are web server software events relevant to supporting incident investigation retained for a minimum of one year?	Yes		Web Server Security	Web Server Auditing and Logging	J.6 IS/IT Incident Management – Analysis	
I.3.2.14.4	Are Web Server and application logs relevant to supporting incident investigation protected against modification, deletion, and/or inappropriate access?	Yes		Web Server Security	Web Server Auditing and Logging	U.1 System Configuration and Hardening Standards	12.4.2 Protection of Log Information 12.4.3 Administrator and Operator Logs
I.3.3	Are compilers, editors or other development tools present in production web server environments?	Yes		Web Server Security	Development Tool Security	I.18 Production Application Vulnerability Monitoring Process	
I.3.6	**Is an API available to clients?**	No		API Security	Scoping	H.3 Logical Access Authorization	

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
I.3.6.1	**Is there a formal security program established to include API security reviews?**	N/A	API not availble for clients	API Security	API Security	I.4 Secure Systems Development Life Cycle (SDLC) Code Reviews	
I.3.6.1.2	Is manual code security testing on APIs performed by qualified personnel with expertise in both development and code security?	N/A		API Security	API Security	I.4 Secure Systems Development Life Cycle (SDLC) Code Reviews	
I.3.6.1.3	Do application security reviews include an API Permission model review?	N/A		API Security	API Security	I.4 Secure Systems Development Life Cycle (SDLC) Code Reviews	
I.3.6.2	Are APIs tested for security weaknesses?	N/A		API Security	API Security	I.3 Application Security SDLC Phases	
I.3.6.3	Can a client manage access to the APIs?	N/A		API Security	API Access		
I.3.6.5	Is Scoped Data encrypted in transit within the API for both request and response?	Yes		API Security	Encryption	D.5 Data Security Policy - Encryption	
I.4	**Are mobile applications that access Scoped Systems and Data developed?**	Yes		Mobile Application Security	Scoping		
I.4.1	Are any actions performed by the mobile application to access, process, transmit or locally store scoped systems and data?	No		Mobile Application Security	Scoping		
I.4.2	Is Dynamic code analysis performed on mobile applications (including fuzzing)?	Yes		Mobile Application Security	Secure Code Analysis	I.9 Secure Code Review	

J. Incident Event and Communications Management

Scoped As: SIG Core 2019 **Progress:** 100% **Tab Automation:** Enable

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 in column F to provide.
- To display the entire contents of the tab, select the word "Disable" in the Tab Automation field at the top of the page.
- Use the Maturity column to identify the Maturity of the question. See the How To Guide for instructions on filling out this field.

Note: There may be gaps in the question number sequence depending on how the issues/outsourcer generated the SIG.

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
J.1	**Is there an established incident management program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the program?**	Yes		Cybersecurity Incident Management	Scoping	J.1 Incident Management – Policy and Procedure Content	16.1.6 Learning from Informtion Security Incidents
J.1.1	Is an Incident / Event Response team available 24x7x365?	Yes		Cybersecurity Incident Management	Cybersecurity Governance	J.1 Incident Management – Policy and Procedure Content	10.1 Nonconformity and Corrective Action Plan 16.1.5 Response to Information Security Events 7.4 Communication
J.2	**Is there a formal Incident Response Plan?**	Yes		Cybersecurity Incident Management	Cybersecurity Incident Response Plan	J.1 Incident Management – Policy and Procedure Content	10.1 Nonconformity and Corrective Action Plan 16.1.4 Assessment and Decision on Information Security Events 16.1.5 Response to Information Security Events 16.1.7 Collection of Evidence 6.1.3 Contact with Authorities 7.4 Communication
J.2.10	Does the Incident Response Plan include guidance for escalation procedure?	Yes		Cybersecurity Incident Management	Cybersecurity Incident Response Plan	J.1 Incident Management – Policy and Procedure Content	10.1 Nonconformity and Corrective Action Plan 16.1.5 Response to Information Security Events 7.4 Communication
J.2.11	Does the Incident Response Plan include procedures to collect and maintain a chain of custody for evidence during incident investigation?	Yes		Cybersecurity Incident Management	Cybersecurity Incident Response Plan	J.1 Incident Management – Policy and Procedure Content	10.1 Nonconformity and Corrective Action Plan 16.1.5 Response to Information Security Events 16.1.7 Collection of Evidence 7.4 Communication
J.2.12	Does the Incident Response Plan include feedback process to ensure those reporting information security events are notified of the results after the issue has been dealt with and closed?	Yes		Cybersecurity Incident Management	Cybersecurity Incident Response Plan	J.7 IS/IT Incident Management – Incident Documentation	10.1 Nonconformity and Corrective Action Plan 16.1.5 Response to Information Security Events 7.4 Communication
J.2.14	Does the Incident Response Plan include actions to be taken in the event of an information security event?	Yes		Cybersecurity Incident Management	Cybersecurity Incident Response Plan	J.1 Incident Management – Policy and Procedure Content	10.1 Nonconformity and Corrective Action Plan 16.1.5 Response to Information Security Events
J.2.15	Does the Incident Response Plan include formal disciplinary process for dealing with those who commit a security breach?	Yes		Cybersecurity Incident Management	Cybersecurity Incident Response Plan	J.11 IS/IT Incident Management – Post Incident	10.1 Nonconformity and Corrective Action Plan 16.1.5 Response to Information Security Events
J.2.16	Does the Incident Response Plan include a process for assessing and executing client and third party notification requirements (legal, regulatory and contractual)?	Yes		Cybersecurity Incident Management	Cybersecurity Incident Response Plan	J.3 Incident Response Communication	10.1 Nonconformity and Corrective Action Plan 16.1.5 Response to Information Security Events 7.4 Communication

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
J.2.19	Does the Incident Response Plan include events relevant to supporting incident investigation regularly reviewed using a specific methodology to uncover potential incidents?	Yes		Cybersecurity Incident Management	Cybersecurity Incident Response Plan	J.1 Incident Management – Policy and Procedure Content	10.1 Nonconformity and Corrective Action Plan 16.1.4 Assessment and Decision on Information Security Events 16.1.5 Response to Information Security Events
J.3	Is the scope of the Incident Management Program defined?	Yes		Cybersecurity Incident Management	Incident Definition	J.1 Incident Management – Policy and Procedure Content	16.1.4 Assessment and Decision on Information Security Events
J.4	**Is there a 24x7x365 staffed phone number available to customers/clients to report security incidents?**	No		Cybersecurity Incident Management	Incident Response Communications	J.4 Information Security/Information Technology (IS/IT) Incident Management – Preparation	
J.4.2	Is the client notified when unauthorized access to Scoped Systems and Data is confirmed?	Yes		Cybersecurity Incident Management	Incident Response Communications	J.7 IS/IT Incident Management – Incident Documentation P.8 Data Protection, Privacy Incident Notification and Response Management	
J.5	**Are events on Scoped Systems or systems containing Scoped Data relevant to supporting incident investigation regularly reviewed using a specific methodology to uncover potential incidents?**	Yes		Security Event Monitoring	Incident Detection	J.1 Incident Management – Policy and Procedure Content J.5 IS/IT Incident Management – Detection	
J.5.1	Is there an automated system to review and correlate log and/or behavioral events (e.g., SIEM)?	Yes		Security Event Monitoring	Incident Detection	J.5 IS/IT Incident Management – Detection	12.4.1 Event Logging
J.5.2	Do personnel monitor security alerts related to Scoped Systems and Data at least daily?	Yes		Security Event Monitoring	Incident Detection	J.5 IS/IT Incident Management – Detection	
J.5.4	Does regular security monitoring include Network IDS events?	Yes		Security Event Monitoring	Incident Detection - NIDS	J.5 IS/IT Incident Management – Detection	
J.5.5	Does regular security monitoring include behavioral activity indicating botnet traffic?	Yes		Security Event Monitoring	Incident Detection - Botnet Traffic	J.5 IS/IT Incident Management – Detection	
J.5.6	Does regular security monitoring include network device security events?	Yes		Security Event Monitoring	Incident Detection - Network Devices	J.5 IS/IT Incident Management – Detection	
J.5.7	Does regular security monitoring include server security events?	Yes		Security Event Monitoring	Incident Detection - Servers	J.5 IS/IT Incident Management – Detection	
J.5.8	Does regular security monitoring include hypervisor security events?	Yes		Security Event Monitoring	Incident Detection - Hypervisors	V.4 Security Review of Hypervisor Configuration	
J.5.9	Does regular security monitoring include application, Web Server, and Database security events?	Yes		Security Event Monitoring	Incident Detection - Applications	J.5 IS/IT Incident Management – Detection	
J.5.10	Does regular security monitoring include malware activity alerts such as uncleaned infections and suspicious activity?	Yes		Security Event Monitoring	Incident Detection - Malware	J.5 IS/IT Incident Management – Detection	
J.6	Is 24x7x365 security monitoring of the hosting environment performed?	Yes		Security Event Monitoring	Incident Detection - Virtualized/ Cloud Environments	J.5 IS/IT Incident Management – Detection	

K. Business Resiliency

Scoped As: SIG Core 2019 **Progress:** 95% **Tab Automation:** Enable

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 in column F to provide.
- To display the entire contents of the tab, select the word "Disable" in the Tab Automation field at the top of the page.
- Use the Maturity column to identify the Maturity of the question. See the How To Guide for instructions on filling out this field.

Note: There may be gaps in the question number sequence depending on how the issues/outsourcer generated the SIG.

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
K.1	**Is there an established business resiliency program that has been approved by management, communicated to appropriate constituents, and an owner to maintain and review the program?**	Yes		Business Resilience Governance	Resilience Program Governance	K.1 Business Resiliency Governance	
K.1.1	Does the business resiliency program include an individual program owner?	Yes		Business Resilience Governance	Resilience Program Governance	K.1 Business Resiliency Governance	
K.1.2	Have appropriate actions been taken to ensure that person(s) working under the Business Resiliency program have or acquire the desired competencies?	Yes		Business Resilience Governance	Business Resilience Roles	K.1 Business Resiliency Governance	
K.1.3	**Does the business resiliency program include a formal annual (or more frequent) executive management review of business continuity key performance indicators, accomplishments, and issues?**	Yes		Business Resilience Governance	Business Resilience Metrics	K.1 Business Resiliency Governance	17.1.3 Verifty, Review and Evaluate Information Security Continuity
K.1.3.1	Does the Business resiliency program's annual review include adequacy of resources including people, technology, facilities, and funding?	Yes		Business Resilience Governance	Business Resilience Metrics	K.1 Business Resiliency Governance	
K.1.3.2	Does the Business resiliency program's annual review include reporting of key program activity and value metrics?	Yes		Business Resilience Governance	Business Resilience Metrics	K.1 Business Resiliency Governance	17.1.3 Verifty, Review and Evaluate Information Security Continuity
K.1.3.3	Does the Business resiliency program's annual review include results of Business Continuity Program audits and reviews, including those of key suppliers and partners where appropriate?	Yes		Business Resilience Governance	Business Resilience Metrics	K.1 Business Resiliency Governance	
K.1.3.4	Does the Business resiliency program's annual review include results of exercising and testing?	Yes		Business Resilience Governance	Business Resilience Metrics	K.1 Business Resiliency Governance	17.1.3 Verifty, Review and Evaluate Information Security Continuity
K.1.3.5	Does the Business resiliency program's annual review include lessons learned and actions arising from disruptive incidents?	Yes		Business Resilience Governance	Business Resilience Metrics	K.1 Business Resiliency Governance	
K.1.4	**Has formal documentation and reference information relevant to the Business Resiliency program and procedures been created?**	Yes		Business Resilience Governance	Business Resilience Documentation	K.1 Business Resiliency Governance	
K.1.4.1	Does Business Resiliency documentation include controls to ensure its availability when and where it is needed?	Yes		Business Resilience Governance	Business Resilience Documentation	K.1 Business Resiliency Governance	
K.1.4.2	Is version and change control managed for Business Resiliency documentation?	Yes		Business Resilience Governance	Business Resilience Documentation	K.1 Business Resiliency Governance	
K.1.5	**Do the products and/or services specified in the scope of this assessment fall within the scope of the Business Resiliency program?**	Yes		Business Resilience Governance	Service Resilience	K.2 Business Impact Analysis (BIA)	
K.1.5.1	Are specific recovery objectives/requirements defined for those products and/or services specified in the scope of this assessment?	Yes		Business Resilience Governance	Service Resilience	K.2 Business Impact Analysis (BIA)	
K.2	**Has a Business Impact Analysis been conducted?**	Yes		Business Continuity Planning	Business Impact Analysis	K.2 Business Impact Analysis (BIA)	17.1.1 Planning Information Security Continuity 17.1.2 Implementing Information Security Continuity 17.1.3 Verifty, Review and Evaluate Information Security Continuity 4.2 Understanding Needs and Expectations of Interested Parties
K.2.1	Does the Business Impact Analysis include validation and/or refresh at least annually?	Yes		Business Continuity Planning	Business Impact Analysis	K.2 Business Impact Analysis (BIA)	17.1.3 Verifty, Review and Evaluate Information Security Continuity
K.2.2	Does the Business Impact Analysis include Business Activity or business process Criticality (high, medium, low or numerical rating) that distinguishes the relative importance of each activity or process?	Yes		Business Continuity Planning	Business Impact Analysis	K.2 Business Impact Analysis (BIA)	
K.2.3	Does the Business Impact Analysis include identification of applications, data, equipment, facilities, personnel, supplies and paper documents necessary for recovery?	Yes		Business Continuity Planning	Business Impact Analysis	K.2 Business Impact Analysis (BIA)	

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
K.2.4	Does the Business Impact Analysis include maximum Acceptable Outage / Maximum Tolerable Period of Disruption for each Business Activity or Business Process?	Yes		Business Continuity Planning	Business Impact Analysis	K.2 Business Impact Analysis (BIA)	
K.2.5	Does the Business Impact Analysis include recovery Time Objectives for all essential application systems, network service, and other resources?	Yes		Business Continuity Planning	Business Impact Analysis	K.2 Business Impact Analysis (BIA)	
K.2.6	Does the Business Impact Analysis include recovery Point Objective for all essential application systems?	Yes		Business Continuity Planning	Business Impact Analysis	K.2 Business Impact Analysis (BIA)	
K.2.7	Does the Business Impact Analysis include impact to clients/customers?	Yes		Business Continuity Planning	Business Impact Analysis	K.2 Business Impact Analysis (BIA)	4.2 Understanding Needs and Expectations of Interested Parties
K.2.8	Does the Business Impact Analysis include capacity to address needs/expectations of all clients/customers?	Yes		Business Continuity Planning	Business Impact Analysis	K.2 Business Impact Analysis (BIA)	4.2 Understanding Needs and Expectations of Interested Parties
K.2.9	Does the Business Impact Analysis include identification of the recovery requirements for information security and the continuity of information security management?	Yes		Business Continuity Planning	Business Impact Analysis	K.2 Business Impact Analysis (BIA)	17.1.1 Planning Information Security Continuity 17.1.2 Implementing Information Security Continuity
K.3	**Is there a formal process focused on identifying and addressing risks of disruptive incidents to business operations?**	Yes		Business Continuity Planning	Operational Risk Assessment	K.3 Risk Assessment	
K.3.1	Do Operational Risk Assessments include identifying risks associated with disruptions to systems, information, people, third parties, and facilities?	Yes		Business Continuity Planning	Operational Risk Assessment	K.3 Risk Assessment	
K.3.2	Do Operational Risk Assessments include analysis of risks identified and determination of those requiring treatments?	Yes		Business Continuity Planning	Operational Risk Assessment	K.3 Risk Assessment	
K.3.3	Do Operational Risk Assessments include taking action on approved treatments?	Yes		Business Continuity Planning	Operational Risk Assessment	K.3 Risk Assessment	
K.4	**Are specific response and recovery strategies defined for the prioritized business activities?**	Yes		Business Continuity Planning	Business Activity Recovery Planning	K.4 Business Activity level Recovery Planning	
K.4.1	Are specific response and recovery strategies defined for critical loss or unavailability of personnel (40% or more)?	Yes		Business Continuity Planning	Business Activity Recovery Planning	K.4 Business Activity level Recovery Planning	
K.4.2	Are specific response and recovery strategies defined for critical loss or unavailability of information and data?	Yes		Business Continuity Planning	Business Activity Recovery Planning	K.4 Business Activity level Recovery Planning	
K.4.3	Are specific response and recovery strategies defined for critical loss or unavailability of information and communication technology?	Yes		Business Continuity Planning	Business Activity Recovery Planning	K.4 Business Activity level Recovery Planning	
K.4.4	Are specific response and recovery strategies defined for critical loss or unavailability of work places/buildings?	Yes		Business Continuity Planning	Business Activity Recovery Planning	K.4 Business Activity level Recovery Planning	
K.4.5	Are specific response and recovery strategies defined for critical loss or unavailability of third party services (e.g., partners and suppliers)?	Yes		Business Continuity Planning	Business Activity Recovery Planning	K.4 Business Activity level Recovery Planning	
K.5	**Are formal business continuity procedures developed and documented?**	Yes		Business Continuity Planning	Business Continuity Procedures	K.4 Business Activity level Recovery Planning	
K.5.1	Do formal business continuity procedures include specific actions to be taken in response to a disruptive event?	Yes		Business Continuity Planning	Business Continuity Procedures	K.4 Business Activity level Recovery Planning	
K.5.2	Do formal business continuity procedures include the continuity of Information security activities and processes (e.g., intrusion detection, vulnerability management, log collection)?	Yes		Business Continuity Planning	Business Continuity Procedures	K.4 Business Activity level Recovery Planning	
K.5.3	Do formal business continuity procedures include the continuity of IT operations activities and processes (e.g., network operations, data center operations, help desk)?	Yes		Business Continuity Planning	Business Continuity Procedures	K.4 Business Activity level Recovery Planning	
K.6	**Has senior management assigned the responsibility for the overall management of critical response and recovery efforts?**	Yes		Business Continuity Planning	Business Recovery Management and Communications	K.1 Business Resiliency Governance	16.1.1 Responsibilities and Procedures 16.1.2 Reporting Information Security Events
K.6.1	Does the overall management of critical response and recovery include a virtual or physical command center where management can meet, organize, and manage emergency operations in a secure setting?	Yes		Business Continuity Planning	Business Recovery Management and Communications	K.1 Business Resiliency Governance	16.1.1 Responsibilities and Procedures
K.6.2	Does the overall management of critical response and recovery include conditions for activating the plan(s), and the associated roles and responsibilities?	Yes		Business Continuity Planning	Business Recovery Management and Communications	K.1 Business Resiliency Governance	16.1.1 Responsibilities and Procedures
K.6.3	Does the overall management of critical response and recovery include roles and responsibilities for those who invoke and execute the plan?	Yes		Business Continuity Planning	Business Recovery Management and Communications	K.1 Business Resiliency Governance	16.1.1 Responsibilities and Procedures

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
K.6.4	Does the overall management of critical response and recovery include alternate and diverse means of communications in the event standard communication channels are unavailable?	Yes		Business Continuity Planning	Business Recovery Management and Communications	K.1 Business Resiliency Governance	16.1.1 Responsibilities and Procedures 16.1.2 Reporting Information Security Events
K.6.5	Does the overall management of critical response and recovery include notification and escalation to customers/clients?	Yes		Business Continuity Planning	Business Recovery Management and Communications	K.1 Business Resiliency Governance	16.1.1 Responsibilities and Procedures 16.1.2 Reporting Information Security Events
K.7	**Is there a periodic (at least annual) review of your Business Resiliency procedures?**	Yes		Business Continuity Planning	Business Continuity Plan Management	K.6 Exercising	
K.7.1	Does periodic review of Business Resiliency procedures include updates to the procedures as necessary after the review?	Yes		Business Continuity Planning	Business Continuity Plan Management	K.1 Business Resiliency Governance K.6 Exercising	
K.7.2	Does periodic review of Business Resiliency procedures include changes in business activities, dependencies and related recovery objectives?	Yes		Business Continuity Planning	Business Continuity Plan Management	K.1 Business Resiliency Governance	
K.7.3	Does periodic review of Business Resiliency procedures include changes in organizational structure and personnel changes?	Yes		Business Continuity Planning	Business Continuity Plan Management	K.1 Business Resiliency Governance	
K.7.4	Does periodic review of Business Resiliency procedures include emerging threats and identified new risks?	Yes		Business Continuity Planning	Business Continuity Plan Management	K.2 Business Impact Analysis (BIA)	
K.7.5	Does periodic review of Business Resiliency procedures include warning and communication procedures and capabilities?	Yes		Business Continuity Planning	Business Continuity Plan Management	K.1 Business Resiliency Governance	
K.7.6	Does periodic review of Business Resiliency procedures include updates from the inventory of IT and telecom assets?	Yes		Business Continuity Planning	Business Continuity Plan Management	K.1 Business Resiliency Governance	
K.8	**Are there any dependencies on critical third party service providers?**	Yes		Business Continuity Planning	Critical Vendors	K.4 Business Activity level Recovery Planning	
K.8.1	**Has contact information for key service provider personnel been documented?**	Yes		Business Continuity Planning	Critical Vendors	K.4 Business Activity level Recovery Planning	
K.8.1.1	Is the contact information for key service provider personnel reviewed and updated at least annually?	Yes		Business Continuity Planning	Critical Vendors	K.4 Business Activity level Recovery Planning	
K.8.2	Have the notification and escalation protocols for key service provider personnel been established?	Yes		Business Continuity Planning	Critical Vendors	K.4 Business Activity level Recovery Planning	
K.8.3	Is communication in the event of a disruption that impacts the delivery of key service provider products and services required?	Yes		Business Continuity Planning	Critical Vendors	K.4 Business Activity level Recovery Planning	
K.8.4	Have processes been implemented to notify key service provider personnel when their business resiliency procedures are modified?	Yes		Business Continuity Planning	Critical Vendors	K.4 Business Activity level Recovery Planning	
K.9	**Is there a formal, documented Information Technology Disaster Recovery exercise and testing program in place?**	Yes		Disaster Recovery Testing	Disaster Recovery Testing Scope	K.6 Exercising	
K.9.1	**Does Information Technology Disaster Recovery testing include specific exercises and tests that address the unavailability of specific IT resources?**	Yes		Disaster Recovery Testing	Disaster Recovery Testing Scope	K.6 Exercising	
K.9.1.1	Does Information Technology Disaster Recovery testing include production data center(s)?	Yes		Disaster Recovery Testing	Disaster Recovery Testing Scope	K.6 Exercising	
K.9.1.2	Does Information Technology Disaster Recovery testing include Data stores?	Yes		Disaster Recovery Testing	Disaster Recovery Testing Scope	K.6 Exercising	
K.9.1.3	Does Information Technology Disaster Recovery testing include recovery supporting critical loss or unavailability of personnel (40% or more)?	Yes		Disaster Recovery Testing	Disaster Recovery Testing Scope	K.6 Exercising	
K.9.1.4	Does Information Technology Disaster Recovery testing include recovery of critical network infrastructure?	Yes		Disaster Recovery Testing	Disaster Recovery Testing Scope	K.6 Exercising	
K.9.2	Does Information Technology Disaster Recovery testing include specific business activity exercises and tests that address the unavailability of specific resources i.e., realistic scenarios?	Yes		Disaster Recovery Testing	Disaster Recovery Testing Scope - Scenarios	K.6 Exercising	
K.9.3	**Are measurable recovery objectives defined for each exercise and test?**	Yes		Disaster Recovery Testing	Disaster Recovery Testing Criteria	K.6 Exercising	
K.9.3.1	Do measurable recovery objectives include Recovery Time Objectives for all essential application systems, network services and other resources?	Yes		Disaster Recovery Testing	Disaster Recovery Testing Criteria	K.6 Exercising	
K.9.3.2	Do measurable recovery objectives include Recovery Point Objectives for all essential application systems?	Yes		Disaster Recovery Testing	Disaster Recovery Testing Criteria	K.6 Exercising	
K.9.4	Are the recovery objective attainment results and the issues identified evaluated with improvement actions identified and acted upon?	Yes		Disaster Recovery Testing	Disaster Recovery Testing Issue Management	K.6 Exercising	

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
K.9.5	**Is there an annual schedule of planned Disaster Recovery and other Business Resiliency exercises and tests?**	Yes		Disaster Recovery Testing	Disaster Recovery Testing Activity Schedule	K.6 Exercising	
K.9.5.1	Do Business Resiliency exercises include evacuation drills?	Yes		Disaster Recovery Testing	Disaster Recovery Testing Activity Schedule	K.6 Exercising	
K.9.5.2	Do Disaster Recovery tests include notification procedure and mechanism tests?	Yes		Disaster Recovery Testing	Disaster Recovery Testing Activity Schedule	K.6 Exercising	
K.9.5.3	Do Disaster Recovery tests include application recovery tests?	Yes		Disaster Recovery Testing	Disaster Recovery Testing Activity Schedule	K.6 Exercising	
K.9.5.4	Do Disaster Recovery tests include remote access tests?	Yes		Disaster Recovery Testing	Disaster Recovery Testing Activity Schedule	K.6 Exercising	
K.9.5.6	Do Disaster Recovery tests include production transaction processing?	Yes		Disaster Recovery Testing	Disaster Recovery Testing Activity Schedule	K.6 Exercising	
K.9.5.7	Do Disaster Recovery tests include typical business volumes / full capacity?	Yes		Disaster Recovery Testing	Disaster Recovery Testing Activity Schedule	K.6 Exercising	
K.9.5.8	Do Business Continuity tests include business relocation testing?	Yes		Disaster Recovery Testing	Disaster Recovery Testing Activity Schedule	K.6 Exercising	
K.9.5.9	Do Disaster Recovery tests include data center failover testing?	Yes		Disaster Recovery Testing	Disaster Recovery Testing Activity Schedule	K.6 Exercising	
K.9.5.10	Are critical service providers included in Disaster Recovery testing?	Yes		Disaster Recovery Testing	Disaster Recovery Testing Activity Schedule	K.6 Exercising	
K.9.5.11	Do Disaster Recovery tests include recovery and continuity of information security controls that may be impacted by a disaster event?	Yes		Disaster Recovery Testing	Disaster Recovery Testing Activity Schedule	K.6 Exercising	
K.9.5.12	Do Business Continuity tests include recovery and continuity of information security operational processes and controls that may be impacted by a non-Disaster Recovery event (e.g., loss of physical work place, reduction in available IS personnel)?	Yes		Disaster Recovery Testing	Disaster Recovery Testing Activity Schedule	K.6 Exercising	
K.9.5.13	Do Business Continuity exercises include recovery and continuity of IT operational processes and controls that may be impacted by a non-Disaster Recovery event (e.g., loss of physical work place, reduction in available IT operations personnel)?	Yes		Disaster Recovery Testing	Disaster Recovery Testing Activity Schedule	K.6 Exercising	
K.9.6	Are the results of exercises conducted internally shared with customers?	No		Disaster Recovery Testing	Customer Participation	K.6 Exercising	
K.9.7	Are joint exercises conducted in partnership with customers?	No		Disaster Recovery Testing	Customer Participation	K.6 Exercising	
K.9.8	Is there an established Business Resiliency exercise scenario addressing cyber resilience?	Yes		Disaster Recovery Testing	Cyber Resilience Scenario Testing	K.6 Exercising	
K.10	Is there a Pandemic / Infectious Disease Outbreak / mass absenteeism Plan?	Yes		Disaster Recovery Testing	Infectious Disease Planning	K.7 INFECTIOUS DISEASE PLANNING	
K.11	**Are any critical subcontractors necessary to provide the scoped services to clients?**	Yes		Business Continuity Planning	Critical Vendors	K.4 Business Activity level Recovery Planning	
K.11.1	Is a critical vendor Dependency Chart or list made available to clients?	Yes		Business Continuity Planning	Critical Vendors	K.4 Business Activity level Recovery Planning	
K.11.5	Do contracts with Critical Service Providers include a penalty or remediation clause for breach of availability and continuity SLAs?	Yes		Business Continuity Planning	Critical Vendors		
K.12	**Could more than one data center contain Scoped Systems and Data at any one time?**	Yes		Capacity Management and Redundancy	Data Center Redundancy		17.2.1 Availability of Information Processing Facilities
K.12.1	**Do the data centers backup one another?**	Yes		Capacity Management and Redundancy	Redundancy mode	K.5 Backup Media Restoration	17.2.1 Availability of Information Processing Facilities

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
K.12.1.1	Are backup data centers' availability mode cold standby?			Capacity Management and Redundancy	Availability Mode		17.2.1 Availability of Information Processing Facilities
K.12.1.2	Are backup data centers' availability mode warm standby?			Capacity Management and Redundancy	Availability Mode		17.2.1 Availability of Information Processing Facilities
K.12.1.3	Are backup data centers' availability mode hot standby?			Capacity Management and Redundancy	Availability Mode		17.2.1 Availability of Information Processing Facilities
K.12.2	Are the failover sites for the underlying infrastructure running on different vendor physical systems?			Capacity Management and Redundancy	Failover		17.2.1 Availability of Information Processing Facilities
K.12.3	Are site failover tests performed at least annually?			Capacity Management and Redundancy	Failover	K.6 Exercising	
K.13	Are networks fully redundant, with at least two network paths to any node, and for every network device, at least one other redundant network device of the same type?	Yes		Capacity Management and Redundancy	Network Redundancy	K.4 Business Activity level Recovery Planning	
K.14	Is there sufficient redundancy capacity to ensure services are not impacted in multi-tenancy environments during peak usage and above?	Yes		Capacity Management and Redundancy	Computing Capacity Management	K.4 Business Activity level Recovery Planning	
K.15	Is there sufficient Volume or Disk partitioning to prevent inadvertent resource bottlenecks from guest operating systems?	Yes		Capacity Management and Redundancy	Disk Capacity Management	K.4 Business Activity level Recovery Planning	
K.16	**Are backups of Scoped Systems and Data performed?**	Yes		Backup and Recovery	Backup Operations	K.5 Backup Media Restoration	12.3.1 Information Backup 17.2.1 Availability of Information Processing Facilities
K.16.1	**Is there a policy or process for the backup of production data?**	Yes		Backup and Recovery	Backup Operations	K.5 Backup Media Restoration	12.3.1 Information Backup 17.2.1 Availability of Information Processing Facilities
K.16.1.1	Are backup media and restoration procedures tested at least annually?	Yes		Backup and Recovery	Backup Operations	K.5 Backup Media Restoration	12.3.1 Information Backup 17.2.1 Availability of Information Processing Facilities
K.16.1.2	Is backup media tracked and reviewed for compliance to data retention/destruction requirements at least annually?	Yes		Backup and Recovery	Backup Operations	K.5 Backup Media Restoration	12.3.1 Information Backup 17.2.1 Availability of Information Processing Facilities
K.16.2	**Are backup and replication errors reviewed and resolved as required?**	Yes		Backup and Recovery	Backup Error Monitoring	K.5 Backup Media Restoration	12.3.1 Information Backup
K.16.2.1	Are backup and replication errors reviewed and resolved at least weekly?	Yes		Backup and Recovery	Backup Error Monitoring	K.5 Backup Media Restoration	12.3.1 Information Backup
K.16.3	**Is backup media stored offsite?**	Yes		Backup and Recovery	Backup Media Transport Security	K.5 Backup Media Restoration	12.3.1 Information Backup
K.16.3.1	Is secure transport used to move backup media offsite?	Yes		Backup and Recovery	Backup Media Transport Security	K.5 Backup Media Restoration	12.3.1 Information Backup
K.16.3.2	Is shipment tracking used when moving backup media offsite?	Yes		Backup and Recovery	Backup Media Transport Security	K.5 Backup Media Restoration	12.3.1 Information Backup
K.16.3.3	Is receipt verification used when moving backup media offsite?	Yes		Backup and Recovery	Backup Media Transport Security	K.5 Backup Media Restoration	12.3.1 Information Backup
K.16.4	Are backups containing Scoped Data stored in an environment where the security controls protecting them are equivalent to the production environment?	Yes		Backup and Recovery	Backup Media Security		12.3.1 Information Backup

L. Compliance

Scoped As: SIG Core 2019 **Progress:** 100% **Tab Automation:** Enable

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 in column F to provide.
- To display the entire contents of the tab, select the word "Disable" in the Tab Automation field at the top of the page.
- Use the Maturity column to identify the Maturity of the question. See the How To Guide for instructions on filling out this field.

Note: There may be gaps in the question number sequence depending on how the issues/outsourcer generated the SIG.

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
L.1	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?	Yes		Compliance Management	Compliance Governance	A.3 Legal, Regulatory and Standards Compliance L.1 Monitoring and Reporting – Compliance/organization	18.1.1 Identification of Applicable Legislation and Contractual Requirements 18.1.2 Intellectual Property Rights
L.2	**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?**	Yes		Compliance Management	Compliance Governance	L.2 Monitoring and Reporting – Compliance Requirement Identification	
L.2.1	Is there a documented process for receiving, monitoring, tracking/logging, and where necessary, implementing changes required to comply with applicable new regulations and regulatory alerts?	Yes		Compliance Management	Compliance Governance	L.2 Monitoring and Reporting – Compliance Requirement Identification	
L.2.2	Are changes required to comply with applicable new regulations and regulatory alerts reported routinely to management and Board of Directors?	Yes		Compliance Management	Compliance Governance		
L.2.3	For employees with access to Scoped Data and/or Scoped Systems, is training on legislative and regulatory requirements provided and updated on a regular basis?	Yes		Compliance Management	Compliance Governance	L.1 Monitoring and Reporting – Compliance/organization	
L.3	**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?**	Yes		Compliance Management	Compliance Organization	L.1 Monitoring and Reporting – Compliance/organization	18.1.1 Identification of Applicable Legislation and Contractual Requirements 18.1.5 Regulation of Cryptographic Controls 18.2.2 Compliance with Security Policies and Standards
L.3.1	**Are audits performed to ensure compliance with applicable statutory, regulatory, contractual or industry requirements?**	Yes		Compliance Management	Compliance Organization	L.1 Monitoring and Reporting – Compliance/organization L.2 Monitoring and Reporting – Compliance Requirement Identification	18.1.1 Identification of Applicable Legislation and Contractual Requirements 18.1.5 Regulation of Cryptographic Controls 18.2.2 Compliance with Security Policies and Standards
L.3.1.1	Does the audit function have independence from the lines of business?	Yes		Compliance Management	Compliance Organization		9.2 Internal Audit
L.3.2	Is there non-audit staff dedicated to compliance and risk responsibilities?	Yes		Compliance Management	Compliance Organization	L.1 Monitoring and Reporting – Compliance/organization	18.1.5 Regulation of Cryptographic Controls 18.2.2 Compliance with Security Policies and Standards
L.4	Are internal management reporting and/or external reporting to government agencies maintained in accordance with applicable law?	Yes		Compliance Management	Compliance Reporting	L.1 Monitoring and Reporting – Compliance/organization	6.1.3 Contact with Authorities
L.5	Are documented policies and procedures maintained for enabling compliance with applicable legal, regulatory or contractual obligations related to cybersecurity requirements?	Yes		Compliance Management	Cybersecurity Regulatory Compliance	L.1 Monitoring and Reporting – Compliance/organization	18.1.4 Privacy and Protection of Personally Identifiable Information
L.6	Is there a records retention policy covering paper & electronic records, including email in support of applicable regulations, standards and contractual requirements?	Yes		Compliance Management	Records Retention		18.1.3 Protection of Records
L.7	**Are business licenses or registrations maintained in all jurisdictions where required?**	Yes		Compliance Management	Business Licenses and Registrations		
L.7.1	Are there policies and procedures to maintain compliance with international requirements for import and/or export of goods or services?	Yes		Compliance Management	International Trade and Export		
L.7.2	Are there policies and procedures to maintain compliance with implemented trade partner restrictions based on international requirements?	Yes		Compliance Management	International Trade and Export		
L.8	Are there policies and procedures to address appropriate due diligence of business partners and business initiatives?	Yes		Compliance Management	Business Due Diligence	L.3 Professional Ethics and Business Practices	

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
L.10	Is there a documented internal compliance and ethics program to ensure professional ethics and business practices are implemented and maintained?	Yes		Business Ethics and Corporate Social Responsibility	Ethics	L.3 Professional Ethics and Business Practices	
L.11	**Has the organization established its standards of conduct concerning integrity and ethical values that are understood by all levels and by outsourced service providers?**	Yes		Business Ethics and Corporate Social Responsibility	Ethics		
L.11.1	Is there a whistleblowing policy and/or separate communication channel procedure to report compliance issues?	Yes		Business Ethics and Corporate Social Responsibility	Ethics	L.3 Professional Ethics and Business Practices	
L.12	**Do employees undergo annual training regarding company expectations related to non-disclosure of insider information, code of conduct, conflicts of interest, and compliance and ethics responsibilities?**	Yes		Business Ethics and Corporate Social Responsibility	Ethics		
L.12.1	Are there policies and procedures to address bribery, corruption or the prohibition of providing monetary offers to government officials, and/or corporate representatives?	Yes		Business Ethics and Corporate Social Responsibility	Anti-Bribery and Anti-Corruption	L.3 Professional Ethics and Business Practices	
L.13	**Are marketing or selling activities conducted directly to Client's customers?**	No		Consumer Protection	Consumer Marketing and Sales	L.4 Marketing and Selling Business Practices	
L.13.1	Is there a documented consumer protection compliance program?	N/A		Consumer Protection	Consumer Marketing and Sales	L.4 Marketing and Selling Business Practices	
L.13.2	Is training conducted for Constituents who have direct customer contact regarding consumer protection compliance responsibilities?	N/A		Consumer Protection	Consumer Marketing and Sales	L.4 Marketing and Selling Business Practices	
L.13.3	Are processes in place to periodically review call center scripts, call monitoring, and/or email marketing to identify compliance issues?	N/A		Consumer Protection	Consumer Marketing and Sales	L.4 Marketing and Selling Business Practices	
L.13.4	Is there an incentive or compensation program for Constituents who directly sell/market to Client customers? If yes please describe in the 'Additional Information' field	N/A		Consumer Protection	Consumer Marketing and Sales		
L.13.5	Are there documented policies and procedures to ensure compliance with applicable laws and regulations including Unfair, Deceptive, or Abusive Acts or Practices?	N/A		Consumer Protection	Complaint Management		
L.14	**Are there direct interactions with your client's customers?**	No		Consumer Protection	Complaint Management	L.4 Marketing and Selling Business Practices	
L.14.1	Is there a documented complaint management function, including reporting within the organization?	N/A		Consumer Protection	Complaint Management	L.4 Marketing and Selling Business Practices	
L.14.2	Is there a documented process to provide periodic summary reports to your applicable Clients regarding types and resolution of complaints?	N/A		Consumer Protection	Complaint Management	L.4 Marketing and Selling Business Practices	
L.14.3	Is there a documented process to receive and respond to complaints, inquiries and requests from trade associations and from government agencies, including state attorneys general?	N/A		Consumer Protection	Complaint Management	L.4 Marketing and Selling Business Practices	
L.14.4	Are calls for telemarketing purposes and/or collections purposes recorded and retained? If yes, please provide the retention period in the 'Additional Information' field.	N/A		Consumer Protection	Complaint Management		
L.14.5	Is there a documented escalation and resolution process to address specific complaints to management and the client?	N/A		Consumer Protection	Complaint Management	L.4 Marketing and Selling Business Practices	
L.14.6	Is a web site(s) maintained or hosted for the purpose of advertising, offering, managing, or servicing accounts, products or services to clients' customers?	N/A		Consumer Protection	Consumer Marketing and Sales		
L.14.7	Are documented terms and conditions, software licensing agreements maintained and available online for enabling compliance with applicable legal, regulatory, and/or contractual obligations related to product or service specifications?	N/A		Consumer Protection	Consumer Marketing and Sales		
L.15	**Are accounts opened, financial transactions initiated or other account maintenance activity (e.g., applying payments, receiving payments, transferring funds, etc.) through either electronic, telephonic, written or in-person requests made on behalf of your clients' customers?**	No		Consumer Protection	Consumer Financial Protection		
L.15.1	Are customer account activities monitored for unusual or suspicious activity?	N/A		Consumer Protection	Consumer Financial Protection	L.1 Monitoring and Reporting – Compliance/organization	
L.16	Are electronic commerce web sites or applications used to transmit, process or store Scoped Systems and Data?	No		eCommerce	Scoping	G.4 Website Setup, Operation and Security	
L.17	Are all transaction details i.e., payment card info and information about the parties conducting transactions, prohibited from being stored in the Internet facing DMZ?	Yes		eCommerce	eCommerce Security		

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
L.18	**Are client audits and/or risk assessments permitted?**	Yes		External Risk Assessment	Client Audit Requirements		
L.18.1	Are onsite audits or risk assessments by clients permitted?	No		External Risk Assessment	Client Audit Requirements		
L.18.4	**Is evidence of internal controls available during a client assessment?**	Yes		External Risk Assessment	Client Audit Requirements		
L.18.4.1	Are system and Network topology and architecture diagrams available during a client risk assessment or audit?	No		External Risk Assessment	Client Audit Requirements	N.2 Network Security – Firewall(s) and/or Other Devices Providing the Same Functionality	
L.18.4.2	Are data flow/System Interface diagrams available during a client risk assessment or audit?	No		External Risk Assessment	Client Audit Requirements	N.2 Network Security – Firewall(s) and/or Other Devices Providing the Same Functionality	
L.18.4.3	Is a list of ports that are open externally available during a client risk assessment or audit?	No		External Risk Assessment	Client Audit Requirements	N.5 Externally Facing Open Administrative Ports	
L.18.4.4	Are system configuration standards available during a client risk assessment or audit?	No		External Risk Assessment	Client Audit Requirements	U.1 System Configuration and Hardening Standards	
L.18.4.5	Are standard operating procedures available during a client risk assessment or audit?	No		External Risk Assessment	Client Audit Requirements	J.2 Incident Response Team – Roles, Responsibilities and Training	
L.19	**Are controls validated by independent, third party auditors or information security professionals?**	Yes		External Risk Assessment	Independent Audits	K.6 Exercising	18.2.1 Independent Review of Information Security
L.19.1	Has a proactive Shared Assessments SCA (Standardized Control Assessment) been performed within the last 12 months?	No		External Risk Assessment	Independent Audits		18.2.1 Independent Review of Information Security
L.19.2	Has a SOC 1 audit been performed within the last 12 months?	N/A		External Risk Assessment	Independent Audits		18.2.1 Independent Review of Information Security
L.19.3	Has a SOC 2 audit been performed within the last 12 months?	Yes		External Risk Assessment	Independent Audits		18.2.1 Independent Review of Information Security
L.19.5	Has an ISO 27001 control assessment been performed within the last 12 months?	Yes		External Risk Assessment	Independent Audits		18.2.1 Independent Review of Information Security
L.19.6	Has an ISO 27017 control assessment been performed within the last 12 months?	No		External Risk Assessment	Independent Audits		18.2.1 Independent Review of Information Security
L.19.7	Has an ISO 27018 control assessment been performed within the last 12 months?	No		External Risk Assessment	Independent Audits		18.2.1 Independent Review of Information Security
L.19.8	Has a NIST 800 53 control assessment been performed within the last 12 months?	No		External Risk Assessment	Independent Audits		18.2.1 Independent Review of Information Security
L.19.9	Has a PCI DSS control assessment been performed within the last 12 months?	N/A		External Risk Assessment	Independent Audits		18.2.1 Independent Review of Information Security
L.19.10	Has a HITRUST CSF control assessment been performed within the last 12 months?	N/A		External Risk Assessment	Independent Audits		18.2.1 Independent Review of Information Security
L.19.11	Has a Multi-tiered cloud computing Security - Singapore (MCTS) assessment been performed within the last 12 months?	No		External Risk Assessment	Independent Audits		18.2.1 Independent Review of Information Security
L.19.12	Have any other audits, risk or control assessments been performed within the last 12 months by an independent firm with transparent standardized audit criteria? If yes, please list/describe in the 'Additional Information' field.	No		External Risk Assessment	Independent Audits		18.2.1 Independent Review of Information Security

M. End User Device Security

Scoped As: SIG Core 2019 **Progress:** 100% **Tab Automation:** Enable

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 in column F to provide.
- To display the entire contents of the tab, select the word "Disable" in the Tab Automation field at the top of the page.
- Use the Maturity column to identify the Maturity of the question. See the How To Guide for instructions on filling out this field.

Note: There may be gaps in the question number sequence depending on how the issues/outsourcer generated the SIG.

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
M.1	**Are End User Devices (Desktops, Laptops, Tablets, Smartphones) used for transmitting, processing or storing Scoped Data?**	No		End User Device Security	Scoping	M.1 End User Device Administrative Activity Logging	11.2.8 Unattended User Equipment 11.2.9 Clear Desk and Clear Screen Policy 12.1.3 Capacity Management
M.1.1	**Are end user device security configuration standards documented?**	N/A		End User Device Security	Security Configuration Standards		
M.1.1.1	Are end user device security configuration standards reviewed and/or updated at least annually to account for any changes in environment, available security features and/or best practices?	N/A		End User Device Security	Security Configuration Standards		
M.1.1.2	Are end user device security reviews performed to validate compliance with documented standards?	N/A		End User Device Security	Security Configuration Standards		
M.1.2	Are all unnecessary/unused services uninstalled or disabled for devices used for accessing, transmitting, processing, or storing Scoped Data on end user devices?	N/A		End User Device Security	End User Device Hardening		12.1.3 Capacity Management
M.1.3	Are all remote access and file sharing services configured to require authentication and encryption on end user devices?	N/A		End User Device Security	End User Device Hardening		6.2.2 Teleworking
M.1.5	Are end user devices configured to lock screens after 15 minutes of inactivity?	N/A		End User Device Security	End User Device Hardening		
M.1.6	Are all available high-risk security patches applied and verified at least monthly on all end-user devices?	N/A		End User Device Security	Patching and Vulnerability Management	G.2 System Patching	
M.1.7	Are all end user device patching exceptions documented and approved by information security or senior management?	N/A		End User Device Security	Patching and Vulnerability Management	G.2 System Patching	
M.1.9	Are all end user device OS versions that no longer have patches released prohibited?	N/A		End User Device Security	Patching and Vulnerability Management		
M.1.10	Are all end user device Operating System and application logs configured to provide sufficient detail to support incident investigation, including successful and failed login attempts and changes to sensitive configuration settings and files?	N/A		End User Device Security	Audit Logs		12.4.1 Event Logging
M.1.15	Are Anti-malware software version and engine upgrade deployment failures reviewed at least weekly for all end user devices?	N/A		End User Device Security	Malware Protection		
M.1.16	Are Activity alerts such as uncleaned infections and suspicious activity reviewed and actioned at least weekly for all end user devices?	N/A		End User Device Security	Malware Protection		
M.1.17	Are defined procedures in place to identify and correct systems without anti-virus at least weekly for all end user devices?	N/A		End User Device Security	Malware Protection		
M.1.18	Are periodic configuration reviews performed at least quarterly and when a change is made to anti-malware standards?	N/A		End User Device Security	Malware Protection		12.2.1 Controls Against Malware
M.1.19	Are application whitelisting, application blacklisting, or restriction of users' ability to install unapproved applications documented and used to prevent the installation of malicious software for all end user devices?	N/A		End User Device Security	Malware Protection		12.2.1 Controls Against Malware 12.5.1 Installation of Software on Operational Systems 12.6.2 Restrictions on Software Installation
M.1.20	Are users required to terminate active sessions when finished on all end user devices?	N/A		End User Device Security	Inactivity Timeout	H.5 Controls for Unattended Systems	11.2.8 Unattended User Equipment 11.2.9 Clear Desk and Clear Screen Policy

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
M.1.21	Is there a requirement to physically secure end user systems when left unattended?	N/A		End User Device Security	Inactivity Timeout	F.3 Secure Workspace Program H.5 Controls for Unattended Systems	11.2.8 Unattended User Equipment 11.2.9 Clear Desk and Clear Screen Policy
M.1.22	**Are Constituents allowed to utilize mobile devices within your environment?**	N/A		Mobile Device Policy and Procedures	Mobile Device Access	F.3 Secure Workspace Program	
M.1.22.1	Can Constituents view Scoped Data using mobile devices?	N/A		Mobile Device Policy and Procedures	Mobile Device Access		
M.1.22.2	Can Constituents process Scoped Data using mobile devices?	N/A		Mobile Device Policy and Procedures	Mobile Device Access		
M.1.22.3	Can Constituents delete Scoped Data using mobile devices?	N/A		Mobile Device Policy and Procedures	Mobile Device Access		
M.1.22.4	Can Constituents store Scoped Data using mobile devices?	N/A		Mobile Device Policy and Procedures	Mobile Device Access		
M.1.22.5	Can Constituents access corporate e-mail using mobile devices?	N/A		Mobile Device Policy and Procedures	Mobile Device Access		
M.1.22.6	Can Constituents connect to Scoped Systems using mobile devices?	N/A		Mobile Device Policy and Procedures	Mobile Device Access		
M.1.23	**Is there a mobile device management program in place that has been approved by management and communicated to appropriate Constituents?**	N/A		Mobile Device Policy and Procedures	Mobile Device Management	F.3 Secure Workspace Program	11.2.6 Security Equipment and Assets Off Premises 6.2.1 Mobile Device Policy
M.1.23.1	Are all mobile devices evaluated as part of the IT Risk Management program?	N/A		Mobile Device Policy and Procedures	Mobile Device Management	F.3 Secure Workspace Program	11.2.6 Security Equipment and Assets Off Premises 6.2.1 Mobile Device Policy
M.1.24	**Are any mobile devices with access to Scoped Data Constituent owned (BYOD)?**	N/A		End User Device Security	BYOD	F.3 Secure Workspace Program	11.2.6 Security Equipment and Assets Off Premises 6.2.1 Mobile Device Policy
M.1.24.1	Are BYOD mobile devices company managed using Mobile Device Management(MDM) technology?	N/A		End User Device Security	BYOD		11.2.6 Security Equipment and Assets Off Premises 6.2.1 Mobile Device Policy
M.1.25	Is a technical solution in place to enforce mobile device security requirements (e.g., PIN, encryption, remote wipe, etc.)?	N/A		Mobile Device Policy and Procedures	Mobile Device Management		11.2.6 Security Equipment and Assets Off Premises 6.2.1 Mobile Device Policy
M.1.26	**Prior to device on-boarding are constituents required to sign a legal agreement which details the obligations and rights related to mobile devices?**	N/A		Mobile Device Policy and Procedures	Mobile Device User Agreement		11.2.6 Security Equipment and Assets Off Premises
M.1.26.1	Does the mobile device user agreement include the owner of data on the mobile device?	N/A		Mobile Device Policy and Procedures	Mobile Device User Agreement		11.2.6 Security Equipment and Assets Off Premises
M.1.26.2	Does the mobile device user agreement include the User's responsibility in ensuring the security of the mobile device?	N/A		Mobile Device Policy and Procedures	Mobile Device User Agreement		11.2.6 Security Equipment and Assets Off Premises
M.1.26.3	Does the mobile device user agreement include the security requirements for Scoped Systems and Data will override user's personal use?	N/A		Mobile Device Policy and Procedures	Mobile Device User Agreement		11.2.6 Security Equipment and Assets Off Premises
M.1.26.4	Does the mobile device user agreement include the support roles and responsibilities?	N/A		Mobile Device Policy and Procedures	Mobile Device User Agreement		11.2.6 Security Equipment and Assets Off Premises
M.1.27	**Is there a process or procedure for responding to mobile device data compromise events?**	N/A		Mobile Device Policy and Procedures	Incident Response Procedures		11.2.6 Security Equipment and Assets Off Premises
M.1.27.1	Does the mobile device incident response process or procedure include remotely wiping the mobile device?	N/A		Mobile Device Policy and Procedures	Incident Response Procedures		11.2.6 Security Equipment and Assets Off Premises
M.1.28	Is there an approved process to support the mobile device lifecycle?	N/A		Mobile Device Policy and Procedures	Mobile Device Management		11.2.6 Security Equipment and Assets Off Premises
M.1.29	**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?**	N/A		Mobile Device Policy and Procedures	Mobile Device Management		11.2.7 Secure Disposal and Re-use of Equipment
M.1.29.1	Does the mobile device offboarding process identify if the Constituent has any legacy devices accessing Scoped Systems and Data?	N/A		Mobile Device Policy and Procedures	Mobile Device Management		11.2.7 Secure Disposal and Re-use of Equipment
M.1.30	Is the identity management system (directory services) integrated with mobile infrastructure to support people joining/leaving/changing roles in the enterprise?	N/A		Mobile Device Policy and Procedures	Mobile Device Management		
M.1.31	Is Mobile Device Management subject to an internal or external audit?	N/A		Mobile Device Policy and Procedures	Mobile Device Management		
M.1.33	Are mobile operating system versions that are deemed end of life permitted to connect to Scoped Systems and Data?	N/A		Mobile Device Policy and Procedures	Mobile Device Management		

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
M.2	**Are personal computers (PCs) used to transmit, process or store Scoped Systems and Data.**	No		Personal Computer Policy and Procedures	Scoping	F.3 Secure Workspace Program	
M.2.1	Is security approval required prior to implementing non-standard PC operating equipment?	N/A		Personal Computer Policy and Procedures	PC Change Management		
M.2.2	Is security approval required prior to implementing freeware or shareware applications on PCs?	N/A		Personal Computer Policy and Procedures	PC Change Management		
M.2.3	Are non-company managed PCs used to connect to the company network?	N/A		Personal Computer Policy and Procedures	BYOD	F.3 Secure Workspace Program	
M.2.4	Is installation of software on company-owned equipment (workstations, mobile devices) restricted to administrators?	N/A		Personal Computer Policy and Procedures	PC Change Management		12.5.1 Installation of Software on Operational Systems 12.6.2 Restrictions on Software Installation
M.3	Are cloud hosting staff technically prevented from accessing the administrative environment via non-managed private devices?	Yes		End User Device Security	Cloud Hosting Staff BYOD	H.3 Logical Access Authorization	

N. Network Security

Scoped As: SIG Core 2019 **Progress:** 100% **Tab Automation:** Enable

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 in column F to provide.
- To display the entire contents of the tab, select the word "Disable" in the Tab Automation field at the top of the page.
- Use the Maturity column to identify the Maturity of the question. See the How To Guide for instructions on filling out this field.

Note: There may be gaps in the question number sequence depending on how the issues/outsourcer generated the SIG.

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
N.1	**Are there external network connections (Internet, extranet, etc.)?**	Yes		Network Policy	Scoping	N.9 Network Security – Authorized Network Traffic	13.1.1 Network Controls 7.5.1 General
N.1.1	**Are there security and hardening standards for network devices, including Firewalls, Switches, Routers and Wireless Access Points (baseline configuration, patching, passwords, Access control)?**	Yes		Network Policy	Hardening Standards	U.1 System Configuration and Hardening Standards	13.1.1 Network Controls 9.1.2 Access to Networks and Network Services
N.1.1.1	Are reviews performed to validate compliance with documented standards at least annually?	Yes		Network Policy	Hardening Standards	U.1 System Configuration and Hardening Standards	
N.1.2	Is there an approval process prior to installing a network device?	Yes		Network Policy	Network Device Change Control	N.9 Network Security – Authorized Network Traffic	
N.1.3	Is security approval required to connect a device on the company network to a non-company network (including the Internet) if it bypasses network security devices (e.g., firewall, IPS, content filter)?	Yes		Network Policy	Network Device Change Control	N.9 Network Security – Authorized Network Traffic	
N.1.5	Does outbound web traffic get scanned for malware, malicious/blacklisted sites and Data policy violations, with any authorized exclusions documented?	Yes		Network Policy	Network Access Control	N.9 Network Security – Authorized Network Traffic	
N.1.6	Is every connection to an external network terminated at a firewall?	Yes		Firewall/ACL Management	Firewall Policy	N.2 Network Security – Firewall(s) and/or Other Devices Providing the Same Functionality	
N.1.9	Do network devices deny all access by default?	Yes		Firewall/ACL Management	ACL Management	J.4 Information Security/Information Technology (IS/IT) Incident Management – Preparation	
N.1.10	Do the firewalls have any rules that permit 'any' network, sub network, host, protocol or port on any of the firewalls (internal or external)?	Yes		Firewall/ACL Management	ACL Management	N.2 Network Security – Firewall(s) and/or Other Devices Providing the Same Functionality	
N.1.12	Is remote access to administrative interfaces configured to require authentication and encryption?	Yes		Secure Configuration	Service Management	H.8 Restrictions and Multifactor Authentication for Remote Access	9.1.2 Access to Networks and Network Services
N.1.13	Are default passwords changed or disabled prior to placing the device into production?	Yes		Secure Configuration	Default Authentication	U.1 System Configuration and Hardening Standards	
N.1.14	Are corporate standardized SNMP Community Strings used, default strings such as 'public' or 'private' removed, and SNMP configured to use the most secure compatible version of the protocol?	Yes		Secure Configuration	Default Authentication		
N.1.15	**Are TACACS+or RADIUS, used to enforce access control policy compliance on all network devices?**	Yes		Remote Access	Access Control		13.1.1 Network Controls
N.1.15.1	Is there a remote access policy for systems transmitting, processing and storing Scoped Systems and Data that has been approved by management and communicated to constituents?	Yes		Remote Access	Policy	H.8 Restrictions and Multifactor Authentication for Remote Access	13.1.1 Network Controls
N.1.15.2	Are split tunneling or bridged internet connections while remotely connected to the company network prohibited by policy and/or technical control?	Yes		Remote Access	Policy		
N.1.15.3	Is only company owned equipment permitted to connect remotely?	Yes		Remote Access	Policy		
N.1.15.4	Are encrypted communications required for all remote connections?	Yes		Remote Access	Encrypted Communications	D.5 Data Security Policy - Encryption	
N.1.15.5	Is multi-factor authentication required for remote network access?	Yes		Remote Access	Multi-factor Authentication	H.8 Restrictions and Multifactor Authentication for Remote Access	
N.1.15.6	Is there a separate network segment or dedicated endpoints for remote access to internal networks?	Yes		Remote Access	VPN Network Segregation	H.8 Restrictions and Multifactor Authentication for Remote Access	
N.1.16	**Is there a process that requires security approval to allow external networks to connect to the company network, and enforces the least privilege necessary?**	Yes		Remote Access	Site to Site VPN Change Control	H.3 Logical Access Authorization	13.1.2 Security of Network Devices

N.1.16.1	Is there a process that requires security approval to allow connections to internal network services from third-party users, and enforces the least privilege necessary?	Yes		Remote Access	Third Party	H.3 Logical Access Authorization	13.1.2 Security of Network Devices
N.1.16.2	Are third party support personnel granted remote network access only upon request, their activity is logged while active, and their access is removed upon completion of support?	Yes		Remote Access	Third Party		13.1.2 Security of Network Devices
N.2	Is remote terminal technology (e.g., RDP, Citrix) used to access Scoped Systems and Data remotely?	Yes		Remote Access	Remote Desktop		
N.3	**Are remote users prevented from copying data to remote non-corporate devices when using remote terminal services?**	Yes		Remote Access	Copy Prevention		
N.3.1	Are all available high-risk security patches applied and verified on network devices?	Yes		Network Device Patch Management	Patching	G.2 System Patching	12.6.1 Management of Technical Vulnerabilities
N.3.2	**Is there sufficient detail contained in network device logs to support incident investigation?**	Yes		Network Device Logging	Logging Detail	N.10 Network Logging	12.4.1 Event Logging 7.5.1 General 7.5.2 Creating and Updating
N.3.2.1	Are network device logs relevant to supporting incident investigation protected against modification, deletion and/or inappropriate access and stored on alternate systems (e.g., SIEM, Syslog, Log Management Service)?	Yes		Network Device Logging	Storage		12.4.1 Event Logging 12.4.2 Protection of Log Information 12.4.3 Administrator and Operator Logs 7.5.1 General 7.5.2 Creating and Updating
N.3.2.2	Are network device events relevant to supporting incident investigation retained for a minimum of one year?	Yes		Network Device Logging	Retention		7.5.1 General
N.3.3	**Are Network Intrusion Detection capabilities employed?**	Yes		Network Security	Network Intrusion Detection/ Prevention	N.3 Network Security – IDS/IPS Attributes	
N.3.3.3	Is the interval between the availability of a new Network IDS/IPS signature update and its deployment in 'Detect' mode no longer than 24 hours?	Yes		Network Security	Network Intrusion Detection/ Prevention	N.3 Network Security – IDS/IPS Attributes	
N.3.3.5	Is there Network IDS/IPS monitoring and alert escalation to security incident response personnel 24x7x365?	Yes		Network Security	Network Intrusion Detection/ Prevention	J.1 Incident Management – Policy and Procedure Content J.5 IS/IT Incident Management – Detection	
N.3.4	**Is there a DMZ environment within the network that transmits, processes or stores Scoped Systems and Data?**	Yes		Network Security	DMZ Security	N.2 Network Security – Firewall(s) and/or Other Devices Providing the Same Functionality	
N.3.4.1	Are DMZ environments limited to only those servers that require access from the Internet?	Yes		Network Security	DMZ Security		
N.3.4.2	Are DMZ environments divided into isolated DMZ network segments for devices that initiate outbound traffic to the Internet and those that only receive inbound traffic?	Yes		Network Security	DMZ Security		
N.3.4.3	Are DMZ environments divided into isolated application and database network segments for internet-facing webpages or other applications with an internet presence?	Yes		Network Security	DMZ Security		
N.4	**Are wireless networking devices connected to networks containing Scoped Systems and Data?**	No		Network Security	Wireless Security	N.7 Unauthorized Wireless Networks	
N.4.1	Is there a wireless policy or program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?	N/A		Network Security	Wireless Security	N.7 Unauthorized Wireless Networks	
N.4.2	Does the Wireless Security Policy require approved and vendor supported wireless access points?	N/A		Network Security	Wireless Security		
N.4.3	Does the Wireless Security Policy prohibit wired and wireless network connections at the same time?	N/A		Network Security	Wireless Security	N.7 Unauthorized Wireless Networks	
N.4.4	Does the Wireless Security Policy require sensitive Wireless networks to be authenticated using multi-factor authentication?	N/A		Network Security	Wireless Security	N.7 Unauthorized Wireless Networks	
N.4.5	Does the Wireless Security Policy require wireless connections to be secured with WPA2, and encrypted using AES or CCMP?	N/A		Network Security	Wireless Security	N.8 Wireless Networks Encryption	
N.4.6	Does the Wireless Security Policy require continuous monitoring and alerting to security personnel, or quarterly scanning for rogue wireless access points?	N/A		Network Security	Wireless Security	N.11 Network Monitoring	
N.5	Are there controls to prevent one client attempting to compromise another client in a resource pooled environment?	Yes		Network Security	Cloud Tenant Segregation Controls	V.4 Security Review of Hypervisor Configuration	

P. Privacy

Scoped As: SIG Core 2019 **Progress:** 100% **Tab Automation:** Enable

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 in column F to provide.
- To display the entire contents of the tab, select the word "Disable" in the Tab Automation field at the top of the page.
- Use the Maturity column to identify the Maturity of the question. See the How To Guide for instructions on filling out this field.

Note: There may be gaps in the question number sequence depending on how the issues/outsourcer generated the SIG.

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
P.1	**Is there collection of, access to, processing of, or retention of any client scoped Data that includes any classification of non-public personal information or personal data of individuals?**	Yes		Privacy Program Management	Scoping	P.1 PRIVACY PROGRAM MANAGEMENT	
P.1.1	Is client scoped Data collected, transmitted, processed, or stored that can be classified as non-public information (NPI), personally identifiable information (PII), or personally identifiable financial information?	Yes		Privacy Program Management	Scoping	P.1 PRIVACY PROGRAM MANAGEMENT	
P.1.2	Is there a designated organizational structure or function responsible for data privacy or data protection as it relates to client-scoped privacy data?	Yes		Privacy Program Management	Organization	P.7 Management of Client-Scoped Privacy Data	
P.1.3	**Is documentation of data flows and/or data inventories maintained for client scoped privacy data based on data or asset classification?**	Yes		Privacy Program Management	Data Management	P.10 Authorizations, Monitoring & Enforcement	18.1.4 Privacy and Protection of Personally Identifiable Information
P.1.3.1	Is there a formalized approval process to review and update data classification definitions and related data flows/data inventories of client scoped privacy data on a periodic basis?	Yes		Privacy Program Management	Data Management	P.7 Management of Client-Scoped Privacy Data	
P.1.4	**Is there a documented Privacy Policy or procedures for the protection of personal information collected, transmitted, processed, or maintained on behalf of the client?**	Yes		Privacy Program Management	Policies and Procedures	P.1 PRIVACY PROGRAM MANAGEMENT P.8 Data Protection, Privacy Incident Notification and Response Management	18.1.4 Privacy and Protection of Personally Identifiable Information
P.1.4.1	Are privacy controls defined and documented which address obligations for the security (confidentiality, integrity, and availability) of the privacy data based on data or asset classification?	Yes		Privacy Program Management	Policies and Procedures		
P.1.4.2	Are there privacy policies and procedures with identified privacy controls that are reviewed and revised at least annually?	Yes		Privacy Program Management	Policies and Procedures	P.7 Management of Client-Scoped Privacy Data	
P.1.4.3	Is there a management procedure maintained to monitor changes in applicable privacy statutory, regulatory or contractual regulations or contractual obligations?	Yes		Privacy Program Management	Policies and Procedures	P.7 Management of Client-Scoped Privacy Data	
P.1.4.4	**Is there a documented privacy policy or procedures maintained for the protection of information collected, transmitted, processed, or maintained on behalf of the client?**	Yes		Privacy Program Management	Policies and Procedures	P.7 Management of Client-Scoped Privacy Data	
P.1.4.5.1	Are privacy risks identified and associated mitigation plans documented in a formal data protection or privacy program plan that is reviewed by management?	Yes		Privacy Program Management	Risk Assessments	P.4 PRIVACY IMPACT RISK ASSESSMENTS	
P.1.4.5.2	Are sufficient resources (e.g. people, time and money) allocated to mitigate identified privacy risks?	Yes		Privacy Program Management	Risk Assessments	P.4 PRIVACY IMPACT RISK ASSESSMENTS	
P.1.4.5.3	Are procedures to assess privacy impact maintained which embed privacy requirements into new systems, applications or devices? (e.g., Privacy by Design) throughout the system lifecycle?	Yes		Privacy Program Management	Risk Assessments	P.4 PRIVACY IMPACT RISK ASSESSMENTS	
P.1.5.1	Is privacy awareness training conducted for new employees at the time of onboarding?	Yes		Privacy Program Management	Training & Awareness	P.3 Privacy Awareness	
P.1.5.2	Is privacy awareness training for employees conducted on an annual basis including acceptance of responsibilities for privacy requirements?	Yes		Privacy Program Management	Training & Awareness	P.3 Privacy Awareness	
P.1.5.3	Are privacy awareness training obligations extended to the organizations subcontractors or third parties?	Yes		Privacy Program Management	Training & Awareness	P.3 Privacy Awareness	
P.1.6.1	Is a process maintained to identify and record any detected or reported unauthorized disclosures of personal information?	Yes		Privacy Program Management	Incident Response Procedures	P.8 Data Protection, Privacy Incident Notification and Response Management	7.5.1 General
P.1.6.2	Is there a process in place to identify and report privacy incidents including notification to external authorities as required by applicable privacy or cyber security law?	Yes		Privacy Program Management	Incident Response Procedures	P.8 Data Protection, Privacy Incident Notification and Response Management	
P.1.6.3	Is there a formal privacy incident communication procedure integrated with the information security incident response and escalation process?	Yes		Privacy Program Management	Incident Response Procedures	P.8 Data Protection, Privacy Incident Notification and Response Management	

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
P.2	**Is conspicuous notice provided in clear and plain language about privacy policies and procedures related to client scoped data?**	Yes		Privacy Notice	Scoping	P.5 DATA COLLECTION, NOTICE, CHOICE & CONSENT	
P.2.1	Do privacy notices identify the purposes for which personal information is collected, used, processed, retained, maintained, and disclosed?	Yes		Privacy Notice	Data Collection	P.5 DATA COLLECTION, NOTICE, CHOICE & CONSENT	
P.2.2	Do privacy notices include the categories of information collected, use of outside data sources, including any categories of affiliates or non-affiliated third parties with whom the personal data is shared?	Yes		Privacy Notice	Policies and Procedures		
P.2.3	Is there an ongoing process to regularly review and update privacy policies and notices on a periodic basis?	Yes		Privacy Notice	Policies and Procedures	P.2 Privacy Organization & Program Maintenance	
P.2.4	Is notice provided at or before point of collection regarding the selling of personal data or sharing of data with third parties for marketing purposes? If yes, please describe the notice in the 'Additional Information' field.	Yes		Privacy Notice	Preference & Consent Management	P.5 DATA COLLECTION, NOTICE, CHOICE & CONSENT	
P.2.5	Are notices communicated to inform individuals regarding awareness of privacy obligations, retention periods of data collected, and opt-out choices applicable to the services?	Yes		Privacy Notice	Preference & Consent Management	P.5 DATA COLLECTION, NOTICE, CHOICE & CONSENT	
P.2.6	**Is a website, mobile, or digital service privacy policy developed, maintained, published, and communicated to users on devices or applications that have access to client-scoped privacy data?**	Yes		Privacy Notice	Data Management		
P.2.6.1	Do Privacy notices identify the Web technology used (e.g. pixels, cookies, web beacons) including description(s) of how technologies are used, and include opt-out mechanisms?	Yes		Privacy Notice	Data Management		
P.3	**Are there documented privacy policies and procedures that address choice and consent based on the statutory, regulatory, or contractual obligations to provide privacy protection for client-scoped privacy data?**	Yes		Privacy Choice and Consent	Scoping	P.5 DATA COLLECTION, NOTICE, CHOICE & CONSENT	
P.3.1	Where the use personal data requires explicit consent, are there mechanisms in place to obtain such consent prior to collection and consistent with the organization's privacy commitments or privacy policy?	Yes		Privacy Choice and Consent	Preference & Consent Management	P.5 DATA COLLECTION, NOTICE, CHOICE & CONSENT	
P.3.2	Are choices offered regarding the collection, use processing, retention, disclosure and disposal of client-scoped personal data communicated?	Yes		Privacy Choice and Consent	Preference & Consent Management	P.5 DATA COLLECTION, NOTICE, CHOICE & CONSENT	
P.3.3	Is there a documented policy or procedure that defines the lawful basis for determining implicit consent for the collection, use, processing, retention, disclosure, and disposal of personal information?	Yes		Privacy Choice and Consent	Preference & Consent Management	P.5 DATA COLLECTION, NOTICE, CHOICE & CONSENT	
P.4	**For client-scoped Data, is personal data collected directly from an individual on behalf of the client or provided to the organization directly by the client?**	Yes		Privacy Data Collection	Scoping	P.10 Authorizations, Monitoring & Enforcement	
P.4.1	Are there documented policies and operating procedures regarding limiting the personal data collected and its use to the minimum necessary?	Yes		Privacy Data Collection	Policies and Procedures	P.7 Management of Client-Scoped Privacy Data	
P.4.2	Are there documented privacy policies and procedures maintained that address data collection based on the statutory, regulatory, or contractual obligations to provide privacy protection for client-scoped privacy data?	Yes		Privacy Data Collection	Policies and Procedures	P.7 Management of Client-Scoped Privacy Data P.10 Authorizations, Monitoring & Enforcement	
P.4.3	Is there a process in place to review and assess any new uses of personal data, confirm authorization or re-gain consent?	Yes		Privacy Data Collection	Policies and Procedures		
P.5	**Are there controls in place to ensure that the collection and usage of personal information is limited and in compliance with applicable law?**	Yes		Use, Retention, & Disposal	Scoping	P.7 Management of Client-Scoped Privacy Data P.10 Authorizations, Monitoring & Enforcement	
P.5.1	Is there a documented records retention policy and process with defined schedules that ensure that Personal Information is retained for no longer than necessary?	Yes		Use, Retention, & Disposal	Policies and Procedures	P.7 Management of Client-Scoped Privacy Data	
P.5.2	Is there a policy and process to limit any secondary use of client Scoped Data unless authorized?	Yes		Use, Retention, & Disposal	Data Management	P.7 Management of Client-Scoped Privacy Data P.10 Authorizations, Monitoring & Enforcement	
P.5.3	Are there control mechanisms in place to de-identify, mask, anonymize, or pseudonymize personal data to prevent loss, theft, misuse or unauthorized access?	Yes		Use, Retention, & Disposal	Data Management	P.7 Management of Client-Scoped Privacy Data	

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
P.5.4	Is there a policy and/or process to limit or prevent the sharing of client-scoped Data with affiliates unless authorized?	Yes		Use, Retention, & Disposal	Data Management	P.7 Management of Client-Scoped Privacy Data P.10 Authorizations, Monitoring & Enforcement	
P.5.5	Is client Scoped Data aggregated, appended, or modeled using outside data sources of personal information?	Yes		Use, Retention, & Disposal	Data Management	P.7 Management of Client-Scoped Privacy Data	
P.5.6	If personal data is kept electronically or processed through automated means, are mechanisms in place to enable data portability for client scoped data? If so describe in 'Additional Information' field.	Yes		Use, Retention, & Disposal	Data Management	P.7 Management of Client-Scoped Privacy Data	
P.6	**If personal data of individuals is retained by your organization, are there processes (e.g., mail, phone, electronic) and procedures to enable individuals to view, access, correct, amend, or delete inaccurate information? If yes, please describe in 'Additional Information' field.**	Yes		Access	Data subject Requests	P.5 DATA COLLECTION, NOTICE, CHOICE & CONSENT P.7 Management of Client-Scoped Privacy Data	
P.6.1	Is there a documented process to reasonably authenticate or verify an individual's request prior to fulfilling their request for access to their personal information?	Yes		Access	Data Subject Requests	P.5 DATA COLLECTION, NOTICE, CHOICE & CONSENT P.7 Management of Client-Scoped Privacy Data	
P.6.2	Is there a process to inform individuals in writing of the reason a request for access to their personal information was denied and the dispute mechanisms if any to challenge as specifically permitted or required by law or regulation?	Yes		Access	Data Subject Requests	P.7 Management of Client-Scoped Privacy Data	
P.7	**Is client scoped data collected by, transmitted to, processed by, accessed by, disclosed to, or retained by third parties?**	Yes		Disclosures to Third Parties	Scoping	P.9 Third Party Privacy Agreements	
P.7.1	Is personal information accessed, disclosed, processed, transmitted or retained by third parties across national borders? If yes, describe and list the countries in 'Additional Information' field.	Yes		Disclosures to Third Parties	Data Management	P.9 Third Party Privacy Agreements P.10 Authorizations, Monitoring & Enforcement	
P.7.2	Do agreements with third parties who have access to or potential access to client Scoped Data address confidentiality, audit, security, and privacy, including but not limited to incident response, ongoing monitoring limitations on data use, limitations on data sharing, return of data, and secure disposal of privacy data?	Yes		Disclosures to Third Parties	Contract Management	P.9 Third Party Privacy Agreements	15.1.2 Addressing Security Within Supplier Agreements 4.2 Understanding Needs and Expectations of Interested Parties
P.7.3	Do contracts or agreements with third parties define the nature, purpose and duration of processing, direction including type of personal data or categories of data that are in scope of the services?	Yes		Disclosures to Third Parties	Contract Management		
P.7.5	**Do fourth-parties, subcontractors, sub-processors, or sub-service organizations have access to or process client scoped data?**	No		Disclosures to Third Parties	Fourth or Nth Parties		
P.7.5.1	Has client consent been obtained for any usage of fourth-parties, subcontractors, sub-processors or sub-service organizations?	N/A		Disclosures to Third Parties	Fourth or Nth Parties		
P.7.5.2	Is a contract maintained with such fourth parties to require each fourth-party, subcontractor, sub-processor, or sub-service organization to adhere to the same legal and contractual requirements that are required by the service organization?	N/A		Disclosures to Third Parties	Fourth or Nth Parties		
P.7.5.3	Has client consent been obtained for any usage of fourth parties, subcontractors, sub-processors or sub-service organizations?	N/A		Disclosures to Third Parties	Fourth or Nth Parties	P.5 DATA COLLECTION, NOTICE, CHOICE & CONSENT P.7 Management of Client-Scoped Privacy Data P.10 Authorizations, Monitoring & Enforcement	
P.7.5.4	Is a contract maintained with fourth parties to require each fourth party, subcontractor, sub-processor, or sub-service organization to adhere to the same legal and contractual requirements that are required by the service organization?	N/A		Disclosures to Third Parties	Fourth or Nth Parties	P.9 Third Party Privacy Agreements	
P.7.6	Are there documented policies, procedures or mechanisms to provide notice, and if required obtain consent for any new, or changed usage of fourth parties, subcontractors, sub-processors, or sub-service organizations?	N/A		Disclosures to Third Parties	Policies and Procedures	P.5 DATA COLLECTION, NOTICE, CHOICE & CONSENT P.7 Management of Client-Scoped Privacy Data	

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
P.7.7	Is there a documented process to obtain and periodically assess compliance with confidentiality and privacy commitments and requirements between client and service provider?	N/A		Disclosures to Third Parties	Policies and Procedures		
P.8	**Is there a documented data protection program with administrative, technical, and physical and environmental safeguards for the protection of client-scoped Data?**	Yes		Security for Privacy	Scoping	P.8 Data Protection, Privacy Incident Notification and Response Management	
P.8.1	Are tests conducted of the effectiveness of the key administrative, technical, physical and environmental safeguards for protecting personal information at least annually?	Yes		Security for Privacy	Testing	K.6 Exercising	
P.8.2	Are mechanisms established so that access to personal information is limited to authorized personnel based upon their assigned roles and responsibilities?	Yes		Security for Privacy	Controls	P.2 Privacy Organization & Program Maintenance P.8 Data Protection, Privacy Incident Notification and Response Management	
P.8.3	Is there a mechanism that informs individuals of the administrative, technical, and physical safeguards taken to protection their personal data?	Yes		Security for Privacy	Policies and Procedures	P.5 DATA COLLECTION, NOTICE, CHOICE & CONSENT	
P.8.4	Is there a vendor risk management program (including ongoing monitoring) maintained to address the security of the client scoped data, that may be accessed, processed, communicated to, or managed by external parties?	Yes		Security for Privacy	Third Party Risk Management	A.5 Third Party Provider Risk Management Program P.2 Privacy Organization & Program Maintenance	15.1.1 Information Security Policy for Supplier Relationships 15.1.2 Addressing Security Within Supplier Agreements
P.8.5	Is there a control to protect personal information stored on portable media or devices from unauthorized access?	Yes		Security for Privacy	Controls		
P.8.6	Is there a process or mechanism to minimize the use of personal data in testing, training and research?	Yes		Security for Privacy	Controls		
P.9	**Is there a documented process to maintain accurate, complete, relevant and timely records of personal information for the purposes identified in the notice?**	Yes		Quality	Scoping	P.7 Management of Client-Scoped Privacy Data	7.5.1 General 7.5.2 Creating and Updating
P.9.1	**Is there a process to respond to individual's requests to review and correct as necessary inaccurate or outdated personal data?**	Yes		Quality	Data Subject Requests	P.7 Management of Client-Scoped Privacy Data	
P.9.1.1	Is there an oversight function or compliance management system maintained that addresses the quality and integrity of personal information?	Yes		Quality	Controls		
P.10	**Is there a data protection function that maintains enforcement and monitoring procedures to address compliance for its privacy obligations for client-scoped privacy data?**	Yes		Monitoring and Enforcement	Scoping	L.2 Monitoring and Reporting – Compliance Requirement Identification P.7 Management of Client-Scoped Privacy Data P.10 Authorizations, Monitoring & Enforcement	
P.10.1	Are there enforcement mechanisms in place to address privacy inquiries, complaints, disputes and recourse for violations of privacy compliance?	Yes		Monitoring and Enforcement	Disputes Resolution	L.2 Monitoring and Reporting – Compliance Requirement Identification P.8 Data Protection, Privacy Incident Notification and Response Management P.10 Authorizations, Monitoring & Enforcement	
P.10.2	Are there policies and processes in place to log and report privacy inquiries, complaints, disputes requests and complaints?	Yes		Monitoring and Enforcement	Disputes Resolution	P.8 Data Protection, Privacy Incident Notification and Response Management P.10 Authorizations, Monitoring & Enforcement	12.4.1 Event Logging
P.10.3	Is an independent dispute mechanism maintained for resolution of privacy disputes? If so, identify the provider in 'Additional Information' field.	Yes		Monitoring and Enforcement	Dispute Resolution	P.8 Data Protection, Privacy Incident Notification and Response Management P.10 Authorizations, Monitoring & Enforcement	
P.10.4	Are applicable registrations, permits, approvals, or adequacy derogations maintained as required by applicable privacy law?	Yes		Monitoring and Enforcement	Compliance	P.10 Authorizations, Monitoring & Enforcement	

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
P.11	**Is client scoped Data collected, transmitted, processed, or retained that can be classified as protected health information (PHI) or other higher healthcare classifications of privacy data?**	No		Protected Health Information	Scoping		
P.11.1	Are there documented policies and procedures to detect and report unauthorized acquisition, use, or disclosure of PHI client scoped data?	N/A		Protected Health Information	Incident Response Procedures		
P.11.2	Are there documented procedures to enable the ability to reasonably amend PHI maintained by the service provider upon request?	N/A		Protected Health Information	Data Management		
P.11.3	Are training records maintained for employees (including management) with access to or potential access to client PHI to meet the privacy and security obligations required by HIPAA? If yes, please describe in 'Additional Information' field.	N/A		Protected Health Information	Training & Awareness		
P.11.4	Is there a business associate contract in place to address obligations for the privacy and security requirements for the services provided to the covered entity?	N/A		Protected Health Information	Contractual Obligations Management	P.9 Third Party Privacy Agreements	
P.12	**Is client-scoped data collected, transmitted, processed or stored that can be classified as consumer report information provided by or to a consumer reporting agency or defined as a covered account under Identity Theft Red Flags Rules?**	No		Consumer and Financial Privacy	Scoping	P.1 PRIVACY PROGRAM MANAGEMENT	
P.12.1	Are policies and procedures for secure disposal of consumer information maintained to prevent the unauthorized access to or use of information in a consumer report or information derived from a consumer report?	N/A		Consumer and Financial Privacy	Policies and Procedures	P.7 Management of Client-Scoped Privacy Data	
P.12.2	Are transactions for Covered Accounts accessed, modified, or processed, including address changes and discrepancies? If yes, please describe in the 'Additional Information' field.	N/A		Consumer and Financial Privacy	Data Management	P.7 Management of Client-Scoped Privacy Data	
P.12.3	Are there documented policies and procedures for identifying and responding to relevant red flags on covered accounts, including address changes and discrepancies?	N/A		Consumer and Financial Privacy	Policies and Procedures		
P.12.4	Is there a documented identify theft prevention program approved by management in place to detect, prevent, and mitigate identify theft?	N/A		Consumer and Financial Privacy	Policies and Procedures	P.1 PRIVACY PROGRAM MANAGEMENT	
P.13	**Is client scoped Data collected, transmitted, processed, or stored that can be classified as European Union covered Personal Data, or Special Categories of Personal Data (e.g., Genetic data, biometric data, health data)?**	Yes		European Privacy & Data Protection	Scoping	P.1 PRIVACY PROGRAM MANAGEMENT	
P.13.1	Are there documented policies and procedures for cross border data flows or transfers of client Scoped Data to the US from other countries; or from EU to other countries?	Yes		European Privacy & Data Protection	Data Transfer	P.1 PRIVACY PROGRAM MANAGEMENT	
P.13.3	If necessary, is your organization registered with the appropriate Data Protection Authorities? If yes, please list which authorities and member countries are in scope for the services in the 'Additional Information' Field.	Yes		European Privacy & Data Protection	Data Protection Authorities	P.1 PRIVACY PROGRAM MANAGEMENT	6.1.3 Contact with Authorities
P.13.4	If required, is there a designated Data Protection Officer? If yes, please identify in the 'Additional Information' field.	Yes		European Privacy & Data Protection	Data Protection Officer	P.1 PRIVACY PROGRAM MANAGEMENT	
P.13.5	Is there a process maintained to remove Personal Data based on the Right to be Forgotten if applicable to the services provided?	Yes		European Privacy & Data Protection	Right to be Forgotten	P.5 DATA COLLECTION, NOTICE, CHOICE & CONSENT	

T. Threat Management

Scoped As: SIG Core 2019 **Progress:** 100% **Tab Automation:** Enable

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 in column F to provide.
- To display the entire contents of the tab, select the word "Disable" in the Tab Automation field at the top of the page.
- Use the Maturity column to identify the Maturity of the question. See the How To Guide for instructions on filling out this field.

Note: There may be gaps in the question number sequence depending on how the issues/outsourcer generated the SIG.

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
T.1	**Are Windows servers used as part of the Scoped Services?**	Yes		Malware Protection	Scoping		
T.1.1	**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?**	Yes		Malware Protection	Anti-Malware Policy	T.1 Anti-malware Protection Policy and Program	12.2.1 Controls Against Malware
T.1.1.1	Does the anti-malware policy or program include defined operating systems that require antivirus?	Yes		Malware Protection	Anti-Malware Policy	T.1 Anti-malware Protection Policy and Program	12.2.1 Controls Against Malware
T.1.1.2	Does the anti-malware policy or program include defined antivirus configuration requirements including required modules/components?	Yes		Malware Protection	Anti-Malware Policy	T.1 Anti-malware Protection Policy and Program	12.2.1 Controls Against Malware
T.1.1.3	Does the anti-malware policy or program prohibit disabling anti-malware with exceptions requiring Security approval and reenablement as soon as possible?	Yes		Malware Protection	Anti-Malware Coverage Exclusions	T.1 Anti-malware Protection Policy and Program	12.2.1 Controls Against Malware
T.1.1.5	Does the anti-malware policy or program require documentation of any folders, applications, and/or processes excluded from anti-malware scanning?	Yes		Malware Protection	Anti-Malware Coverage Exclusions	T.1 Anti-malware Protection Policy and Program	12.2.1 Controls Against Malware
T.1.1.6	Does the approved anti-malware policy or program mandate an interval between the availability of a new anti-malware signature update and its deployment no longer than 24 hours?	Yes		Malware Protection	Anti-Malware Policy	T.1 Anti-malware Protection Policy and Program	12.2.1 Controls Against Malware
T.1.1.8	Are anti-malware standards reviewed and/or updated at least annually to account for new security features and threats?	Yes		Malware Protection	Anti-Malware Policy	T.1 Anti-malware Protection Policy and Program	12.2.1 Controls Against Malware
T.1.1.9	Are Anti-malware software version and engine upgrade deployment failures reviewed at least weekly?	Yes		Malware Protection	Anti-Malware Operations		12.2.1 Controls Against Malware
T.1.1.10	Is there a defined procedure to identify and correct systems without anti-malware software, performed at least weekly?	Yes		Malware Protection	Anti-Malware Operations	T.2 Virus Protection (Servers) T.3 Virus Protection (Workstations)	12.2.1 Controls Against Malware
T.1.1.11	Does the anti-malware policy or program require a periodic configuration review performed at least quarterly and when a change is made to anti-malware standards?	Yes		Malware Protection	Anti-Malware Policy	T.1 Anti-malware Protection Policy and Program	12.2.1 Controls Against Malware
T.2	**Is there a vulnerability management policy or program that has been approved by management, communicated to appropriate constituent and an owner assigned to maintain and review the policy?**	Yes		Vulnerability Management	Vulnerability Management Policy	T.4 Application Vulnerability Assessments/Ethical Hacking	12.6.1 Management of Technical Vulnerabilities
T.2.2	Are vulnerabilities documented and tracked to remediation?	Yes		Vulnerability Management	Vulnerability Remediation	T.4 Application Vulnerability Assessments/Ethical Hacking	12.6.1 Management of Technical Vulnerabilities
T.2.3	Are exceptions and risk mitigation strategies tracked and approved by the Security group?	Yes		Vulnerability Management	Vulnerability Remediation	T.1 Anti-malware Protection Policy and Program	12.6.1 Management of Technical Vulnerabilities
T.2.4	**Are network Vulnerability Scans performed against internal networks and systems?**	Yes		Vulnerability Management	Vulnerability Scans: Internal	T.4 Application Vulnerability Assessments/Ethical Hacking	12.6.1 Management of Technical Vulnerabilities
T.2.4.1	Do network Vulnerability Scans occur at least Monthly?	Yes		Vulnerability Management	Vulnerability Scans: Internal	T.4 Application Vulnerability Assessments/Ethical Hacking	12.6.1 Management of Technical Vulnerabilities
T.2.4.2	Do network Vulnerability Scans occur after a significant change?	Yes		Vulnerability Management	Vulnerability Scans: Internal	T.4 Application Vulnerability Assessments/Ethical Hacking	12.6.1 Management of Technical Vulnerabilities
T.2.5	**Are network vulnerability scans performed against internet-facing networks and systems?**	Yes		Vulnerability Management	Vulnerability Scans External	T.4 Application Vulnerability Assessments/Ethical Hacking	12.6.1 Management of Technical Vulnerabilities
T.2.5.1	Do network Vulnerability Scans occur at least Monthly?	Yes		Vulnerability Management	Vulnerability Scans External	T.4 Application Vulnerability Assessments/Ethical Hacking	12.6.1 Management of Technical Vulnerabilities
T.2.5.2	Do network Vulnerability Scans occur after a significant change?	Yes		Vulnerability Management	Vulnerability Scans External	T.4 Application Vulnerability Assessments/Ethical Hacking	12.6.1 Management of Technical Vulnerabilities
T.2.6	**Are penetration tests performed?**	Yes		Vulnerability Management	Penetration Testing	T.4 Application Vulnerability Assessments/Ethical Hacking	12.6.1 Management of Technical Vulnerabilities
T.2.6.1	Is penetration testing performed at least annually?	Yes		Vulnerability Management	Penetration Testing	T.4 Application Vulnerability Assessments/Ethical Hacking	12.6.1 Management of Technical Vulnerabilities
T.2.6.3	Are Penetration Tests performed by independent trained and experienced personnel?	Yes		Vulnerability Management	Penetration Testing	T.4 Application Vulnerability Assessments/Ethical Hacking	12.6.1 Management of Technical Vulnerabilities

T.2.6.4	Do penetration tests procedures include manual in addition to automated procedures?	Yes		Vulnerability Management	Penetration Testing	T.4 Application Vulnerability Assessments/Ethical Hacking	12.6.1 Management of Technical Vulnerabilities
T.2.6.5	Is penetration testing performed on external systems from the Internet?	Yes		Vulnerability Management	Penetration Testing	T.4 Application Vulnerability Assessments/Ethical Hacking T.5 Technical Compliance Checking – Vulnerability Testing and Remediation	12.6.1 Management of Technical Vulnerabilities
T.2.6.9	Are web applications included in Penetration Tests?	Yes		Vulnerability Management	Penetration Testing	T.4 Application Vulnerability Assessments/Ethical Hacking	12.6.1 Management of Technical Vulnerabilities
T.2.6.10	Are network and system details provided to the tester (White-Box Test) in Penetration Tests?	Yes		Vulnerability Management	Penetration Testing		12.6.1 Management of Technical Vulnerabilities
T.2.6.11	Are Penetration Testing issues risk-ranked for importance to the system and vulnerability identified?	Yes		Vulnerability Management	Penetration Testing	T.4 Application Vulnerability Assessments/Ethical Hacking	12.6.1 Management of Technical Vulnerabilities
T.2.6.12	Are Penetration Testing issues documented and tracked to remediation?	Yes		Vulnerability Management	Penetration Testing	T.4 Application Vulnerability Assessments/Ethical Hacking	12.6.1 Management of Technical Vulnerabilities
T.2.6.13	Are Penetration Testing exceptions and risk mitigation strategies tracked and approved by the security group?	Yes		Vulnerability Management	Penetration Testing	T.4 Application Vulnerability Assessments/Ethical Hacking	12.6.1 Management of Technical Vulnerabilities
T.3	Are there policies and processes to secure threat and vulnerability assessment tools and the data they collect?	Yes		Vulnerability Management	Security Tools	T.4 Application Vulnerability Assessments/Ethical Hacking	

U. Server Security

Scoped As: SIG Core 2019 **Progress:** 100% **Tab Automation:** Enable

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 in column F to provide.
- To display the entire contents of the tab, select the word "Disable" in the Tab Automation field at the top of the page.
- Use the Maturity column to identify the Maturity of the question. See the How To Guide for instructions on filling out this field.

Note: There may be gaps in the question number sequence depending on how the issues/outsourcer generated the SIG.

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
U.1	**Are Servers used for transmitting, processing or storing Scoped Data?**	Yes		Server Security	Scoping	U.1 System Configuration and Hardening Standards	
U.1.1	**Are server security configuration standards documented and based on external industry or vendor guidance?**	Yes		Server Security Configuration Management	Server Security Configuration Standards	U.1 System Configuration and Hardening Standards	
U.1.1.1	Are server security standards reviewed and/or updated at least annually to account for any changes in environment, available security features and/or leading practices?	Yes		Server Security Configuration Management	Server Security Configuration Standards	U.1 System Configuration and Hardening Standards	
U.1.1.2	**Are server security configuration reviews performed regularly to validate compliance with documented standards?**	Yes		Server Security Configuration Management	Server Security Configuration Reviews	U.1 System Configuration and Hardening Standards	
U.1.1.2.1	Are server security configuration reviews performed to validate compliance with documented standards at least annually?	Yes		Server Security Configuration Management	Server Security Configuration Reviews	U.1 System Configuration and Hardening Standards	
U.1.2	**Are all servers configured according to security standards as part of the build process?**	Yes		Server Security Configuration Management	Server Build Security Configuration	U.1 System Configuration and Hardening Standards	
U.1.2.1	Are all unnecessary/unused services uninstalled or disabled on all servers?	Yes		Server Security Configuration Management	Network and System Services	U.1 System Configuration and Hardening Standards	
U.1.2.2	Are all remote access and file sharing services configured to require authentication and encryption on all servers?	Yes		Server Security Configuration Management	Network and System Services	U.1 System Configuration and Hardening Standards	
U.1.2.3	Is data on a separate drive than the Operating System executables/binaries on all servers?	Yes		Server Security Configuration Management	Volume Security	U.1 System Configuration and Hardening Standards	
U.1.2.4	Are all servers configured to log users out after 15 minutes of inactivity?	Yes		Server Security Configuration Management	Session Time-Out	U.1 System Configuration and Hardening Standards	
U.1.2.5	Are vendor default passwords removed, disabled or changed prior to placing any device or system into production?	Yes		Server Security Configuration Management	Password Management	U.1 System Configuration and Hardening Standards	
U.1.3	**Is sufficient detail contained in Operating System and application logs to support security incident investigations (at a minimum, successful and failed login attempts, and changes to sensitive configuration settings and files)?**	Yes		Server Security Configuration Management	Audit Logs	U.1 System Configuration and Hardening Standards	12.4.1 Event Logging 7.5.1 General 7.5.2 Creating and Updating
U.1.3.1	Are operating system and application events relevant to supporting incident investigation retained for a minimum of one year?	Yes		Server Security Configuration Management	Audit Logs	U.1 System Configuration and Hardening Standards	7.5.1 General
U.1.3.2	Are operating system and application logs relevant to supporting incident investigation protected against modification, deletion and/or inappropriate access?	Yes		Server Security Configuration Management	Audit Logs	U.1 System Configuration and Hardening Standards	12.4.2 Protection of Log Information 12.4.3 Administrator and Operator Logs 7.5.1 General 7.5.2 Creating and Updating
U.1.3.3	Are operating system and application events relevant to supporting incident investigation stored on alternate systems?	Yes		Server Security Configuration Management	Audit Logs	U.1 System Configuration and Hardening Standards	12.4.2 Protection of Log Information 12.4.3 Administrator and Operator Logs
U.1.4	Is an alert generated if removable media (floppy disk, recordable CD, USB drive) is used on servers?	Yes		Server Security Configuration Management	Audit Logs	U.1 System Configuration and Hardening Standards	

U.1.5	**Are all systems and applications patched regularly?**	Yes		Server Patching	Patching Cadence	U.1 System Configuration and Hardening Standards	
U.1.5.1	Are all available high-risk security patches applied and verified at least monthly on all server platforms?	Yes		Server Patching	Patching Cadence	U.1 System Configuration and Hardening Standards	
U.1.5.6	Are all server patching exceptions necessary, documented and approved?	Yes		Server Patching	Patching Exception Management	U.1 System Configuration and Hardening Standards	
U.1.5.8	Are there any Operating System versions in use within the Scoped Services that no longer have patches released? If yes, please describe in the 'Additional Information' section.	Yes		Server Patching	Patching Operations	U.1 System Configuration and Hardening Standards	
U.1.6	**Is Unix or Linux used as part of the Scoped Services?**	No		Unix/Linux Security	Scoping	U.1 System Configuration and Hardening Standards	
U.1.6.1	Are users required to 'su' or 'sudo' into root?	N/A		Unix/Linux Security	Root/Administrator Authentication	U.1 System Configuration and Hardening Standards	
U.1.6.2	Does remote su/root access require multi-factor authentication?	N/A		Unix/Linux Security	Multi-factor SU/Root	U.1 System Configuration and Hardening Standards	
U.1.7	**Are AS/400s used as part of the Scoped Services?**	No		AS/400 Security	Scoping	U.1 System Configuration and Hardening Standards	
U.1.7.1	Are group profile assignments based on constituent role?	N/A		AS/400 Security	Role-Based Group Profile	U.1 System Configuration and Hardening Standards	
U.1.7.2	Are group profile assignments approved?	N/A		AS/400 Security	Group Profile Approval	U.1 System Configuration and Hardening Standards	
U.1.8	**Are Mainframes used as part of the Scoped Services?**	No		Mainframe Security	Scoping	U.1 System Configuration and Hardening Standards	
U.1.8.2	Are ESM (RACF) and inherent security configuration settings configured to support mainframe access control standards and requirements?	N/A		Mainframe Security	Access Control Subsystem Configuration Management	U.1 System Configuration and Hardening Standards	
U.1.8.3	Is authentication required for access to any mainframe transaction or database system?	N/A		Mainframe Security	Transaction or Database Authentication	U.1 System Configuration and Hardening Standards	
U.1.9	**Are Hypervisors used to manage systems used to transmit, process or store Scoped Data?**	Yes		Hypervisor and Virtualization Security	Hypervisor Security	U.1 System Configuration and Hardening Standards	12.4.1 Event Logging 12.4.2 Protection of Log Information 12.4.3 Administrator and Operator Logs 7.5.1 General
U.1.9.1	Are Hypervisor hardening standards applied on all Hypervisors?	Yes		Hypervisor and Virtualization Security	Hypervisor Security	U.1 System Configuration and Hardening Standards	
U.1.9.2	Are Hypervisor Standard builds/security compliance checks required?	Yes		Hypervisor and Virtualization Security	Hypervisor Security	U.1 System Configuration and Hardening Standards	
U.1.9.3	Are Hypervisors kept up to date with current patches?	Yes		Hypervisor and Virtualization Security	Hypervisor Security	U.1 System Configuration and Hardening Standards	
U.1.9.4	Are unnecessary/unused Hypervisor services turned off?	Yes		Hypervisor and Virtualization Security	Hypervisor Security	U.1 System Configuration and Hardening Standards	
U.1.9.5	Is sufficient information in Hypervisor logs to evaluate incidents?	Yes		Hypervisor and Virtualization Security	Hypervisor Security	U.1 System Configuration and Hardening Standards	12.4.1 Event Logging 7.5.1 General
U.1.9.6	Are Hypervisor logs retained for a minimum of one year?	Yes		Hypervisor and Virtualization Security	Hypervisor Security	U.1 System Configuration and Hardening Standards	12.4.1 Event Logging 7.5.1 General
U.1.9.8	Are Hypervisor audit logs stored on alternate systems?	Yes		Hypervisor and Virtualization Security	Hypervisor Security	U.1 System Configuration and Hardening Standards	12.4.2 Protection of Log Information 12.4.3 Administrator and Operator Logs
U.1.9.9	Are Hypervisor audit logs protected against modification, deletion and/or inappropriate access?	Yes		Hypervisor and Virtualization Security	Hypervisor Security	U.1 System Configuration and Hardening Standards	12.4.2 Protection of Log Information 12.4.3 Administrator and Operator Logs
U.1.9.10	Does the Hypervisor system lock accounts after 3-5 invalid login attempts?	Yes		Hypervisor and Virtualization Security	Hypervisor Security	U.1 System Configuration and Hardening Standards	
U.1.9.11	Is administrative access restricted to Hypervisor management interfaces?	Yes		Hypervisor and Virtualization Security	Hypervisor Security	U.1 System Configuration and Hardening Standards	
U.1.9.12	Are unneeded Hypervisor services (e.g., file-sharing between the guest and the host operating system) disabled?	Yes		Hypervisor and Virtualization Security	Hypervisor Security	U.1 System Configuration and Hardening Standards	

U.1.9.13	Does the Hypervisor have introspection capabilities to monitor the security of each guest operating system?	Yes		Hypervisor and Virtualization Security	Guest OS Security	U.1 System Configuration and Hardening Standards	
U.1.9.14	Does the Hypervisor have introspection capabilities to monitor the security of activity taking place between each guest operating system?	Yes		Hypervisor and Virtualization Security	Virtual Network Security	U.1 System Configuration and Hardening Standards	
U.1.9.15	Are separate network VLANs for host operating system communication with guest operating systems configured in the Hypervisor?	Yes		Hypervisor and Virtualization Security	Virtual Network Security	U.1 System Configuration and Hardening Standards	
U.1.9.16	Do guest operating systems communicate on separate VLAN's from other Guest operating systems that they do not need to communicate with?	Yes		Hypervisor and Virtualization Security	Virtual Network Security	U.1 System Configuration and Hardening Standards	
U.1.9.17	Is the host operating system management interface on a separate network than those used by guest operating systems?	Yes		Hypervisor and Virtualization Security	Virtual Network Security	U.1 System Configuration and Hardening Standards	
U.1.9.18	Is two factor authentication required for access to the administrative interfaces?	Yes		Hypervisor and Virtualization Security	Hypervisor Security	U.1 System Configuration and Hardening Standards	
U.1.9.19	Is there an approval process before VMs can be created to avoid VM sprawl?	Yes		Hypervisor and Virtualization Security	Virtual Machine Management	U.1 System Configuration and Hardening Standards	
U.1.9.20	Is migration of VMs logged, including source and target systems, time, user?	Yes		Hypervisor and Virtualization Security	Virtual Machine Management	U.1 System Configuration and Hardening Standards	
U.1.9.22	Do all VMs in the same host share the same system sensitivity level grouping (development and production not present on the same host)?	Yes		Hypervisor and Virtualization Security	Virtual Machine Management	U.1 System Configuration and Hardening Standards	
U.1.10	**Are Containers (e.g., Docker, Kubernetes, OpenShift) used to process or store Scoped Data?**	No		Container Security	Scoping	U.1 System Configuration and Hardening Standards	
U.1.10.1	Can clients prohibit containers from being used on scoped systems with sensitive or confidential information?	N/A		Container Security	Prohibition	U.1 System Configuration and Hardening Standards	
U.1.10.2	Is there a Data Container Security policy approved by management, communicated to constituents and an owner to maintain and review?	N/A		Container Security	Container Security Policy	U.1 System Configuration and Hardening Standards	
U.1.10.3	Does the Data Container Security policy include security requirements implemented as part of the container build process?	N/A		Container Security	Container Security Policy	U.1 System Configuration and Hardening Standards	
U.1.10.4	Does the Data Container Security policy require Data Containers on the same host share the same risk and data classification?	N/A		Container Security	Container Security Policy	U.1 System Configuration and Hardening Standards	
U.1.10.5	Does the Data Container Security policy require external Container images to be signed and originate from a trusted registry?	N/A		Container Security	Container Security Policy	U.1 System Configuration and Hardening Standards	
U.1.10.6	Does the Data Container Security policy ensure Containers are scanned for vulnerabilities and identified vulnerabilities are remediated?	N/A		Container Security	Container Security Policy	U.1 System Configuration and Hardening Standards	
U.1.10.7	Does the Data Container Security policy require that Seccomp profiles are enabled to reduce the number of potentially risky usable system calls?	N/A		Container Security	Container Security Policy	U.1 System Configuration and Hardening Standards	
U.1.10.8	Does the Data Container Security policy require that an Authorization Plug-In is enabled?	N/A		Container Security	Container Security Policy	U.1 System Configuration and Hardening Standards	
U.1.10.9	Does the Data Container Security policy require that Control Groups are enabled to reduce the kernel and system resources that a container can consume?	N/A		Container Security	Container Security Policy	U.1 System Configuration and Hardening Standards	
U.1.10.10	Does the Data Container Security policy require that Linux User Namespace Support is enabled to reduce the kernel and system resources that a container can access?	N/A		Container Security	Container Security Policy	U.1 System Configuration and Hardening Standards	
U.1.10.11	Are Vulnerability Scans performed against all Containers using tools that can inspect the contents of Containers?	N/A		Container Security	Vulnerability Management		

V. Cloud Hosting

Scoped As: SIG Core 2019 **Progress:** 100% **Tab Automation:** Enable

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 in column F to provide.
- To display the entire contents of the tab, select the word "Disable" in the Tab Automation field at the top of the page.
- Use the Maturity column to identify the Maturity of the question. See the How To Guide for instructions on filling out this field.

Note: There may be gaps in the question number sequence depending on how the issues/outsourcer generated the SIG.

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
V.1	**Are Cloud Hosting services (IaaS) provided?**	No		Cloud Hosting	Cloud Service Model	V.1 Service and Deployment Models	
V.1.1	**Is there an Internet-accessible self-service portal available that allows clients to configure security settings and view access logs, security events and alerts?**	N/A		Cloud API	Scoping	J.5 IS/IT Incident Management – Detection	7.5.1 General
V.1.1.8	Does the API have the ability to alert, block or lock based on rate limit?	N/A		Cloud API	Cloud Security Configuration		
V.2	**Are Cloud Hosting services subcontracted?**	N/A		Cloud Hosting Organization	Subcontracted Cloud Services	V.2 Nested Service Provider Relationships	
V.2.1	Is there a full time internal security team assigned to protecting the cloud hosting infrastructure?	N/A		Cloud Hosting Organization	Information Security Team Responsibilities	V.3 Cloud Audit Program	
V.3	**Is there a management approved process to ensure that backup image snapshots containing Scoped Data are authorized by Outsourcer prior to being snapped?**	N/A		Configuration Management	Backup Image Management	V.1 Service and Deployment Models	
V.3.1	Are backup image snapshots containing Scoped Data stored in an environment where the security controls protecting them are commensurate with the production environment?	N/A		Configuration Management	Backup Image Management	V.1 Service and Deployment Models	
V.3.2	Can backup image versions be electronically signed to ensure integrity?	N/A		Configuration Management	Backup Image Management	V.1 Service and Deployment Models	
V.4	**Is the Assessee responsible for deploying patches to the live guest Operating Systems?**	N/A		Configuration Management	Patch Management	V.2 Nested Service Provider Relationships	
V.4.1	Is the Assessee responsible for ensuring the live Guest Operating Systems remain hardened?	N/A		Configuration Management	Periodic Configuration Review	V.2 Nested Service Provider Relationships	
V.4.2	Is the Assessee responsible for deploying patches to all application server components (e.g., web server, mail server, databases)?	N/A		Configuration Management	Patch Management	V.2 Nested Service Provider Relationships	
V.4.3	Is the Assessee responsible for ensuring all application server components (e.g. web server, mail server, databases) remain hardened?	N/A		Configuration Management	Periodic Configuration Review	V.2 Nested Service Provider Relationships	
V.5	**Are default hardened base virtual images applied to virtualized operating systems?**	N/A		Configuration Management	Periodic Configuration Review	V.1 Service and Deployment Models	
V.5.1	Are default hardened base virtual images based on a publicly distributed industry, vendor, or government-recognized configuration standard?	N/A		Configuration Management	Periodic Configuration Review	V.1 Service and Deployment Models	
V.5.2	**Is the Service Provider responsible for ensuring the Guest Operating System Base Images are hardened to the latest standards?**	N/A		Configuration Management	Base Image Management	V.1 Service and Deployment Models	
V.5.2.1	Can a client supply their own default base virtual image for Guest Operating Systems?	N/A		Configuration Management	Base Image Management	V.1 Service and Deployment Models	
V.5.3	Is the Service Provider responsible for deploying patches to the Guest Operating System Base Images?	N/A		Configuration Management	Patch Management	V.2 Nested Service Provider Relationships	
V.6	**Does the Cloud Hosting Provider provide independent audit reports (e.g., Service Operational Control - SOC) for their cloud hosting services?**	N/A		Independent Oversight	Audit Reports	V.3 Cloud Audit Program	
V.6.1	Are independent audit reports provided by the Cloud Hosting Provider valid for a 12-month period, completed within the last 12 months, performed by a certified audit firm, and free of qualified opinion?	N/A		Independent Oversight	Audit Reports	V.3 Cloud Audit Program	
V.6.2	**Is the Cloud Service Provider certified by an independent third party for compliance with domestic or international control standards (e.g., the National Institute of Standards and Technology - NIST, the International Organization for Standardization - ISO)?**	N/A		Independent Oversight	Audit Reports	V.3 Cloud Audit Program	
V.6.2.1	Are any certifications of the Cloud Service Provider's environment current, performed by a certified audit firm, and have they been reassessed within the last 12 months?	N/A		Independent Oversight	Audit Reports	V.3 Cloud Audit Program	
V.6.3	**Can clients run their own vulnerability scans against their own cloud environment?**	N/A		Independent Oversight	Client-Managed Security	V.3 Cloud Audit Program	

Ques Num	Question/Request	Response	Additional Information	Category	Sub-category	SCA Reference	ISO 27002:2013 Relevance
V.6.3.1	Can clients procure their own network security services (e.g., Firewall, IDS, IPS, WAF)?	N/A		Independent Oversight	Client-Managed Security	V.3 Cloud Audit Program	

Formula Notes

Column	Description
A ***<Serial No>***	This is a unique record for a question. This value is sequential starting with one on Tab A to the end of questions on last tab. Any row that is not a question will not have a number. The highest value used as a unique identifier is located on this tab in cell D35 (below).
A4	Calculates the highest serial number on the tab. This tab cell C22 identifies the highest serial number used so new question serial numbers can be used. Retired serial numbers are never re-used.
B **Conditional Formatting**	The question text will be bold if the question has a child question and tab automation is enabled. Questions not bold have no children or tab automation is disabled.
D **Conditional Formatting** ***<Response>***	The conditional formatting looks in column J and U to determine the background of the cell. If the value in column J =1, conditional formatting sets the background to a hash (no response required) to indicated the top of a table question. If the value in column U = 1 the background will be green indicating a "Yes" response. If the value in column U = 2 than the background will turn orange indicating a "No" response. If the value in column U = 3 the background turns violet to indicate an N/A response. The default background is light blue.
E **Conditional Formatting** ***<Additional Information>***	The conditional formatting looks in column J. If the value in column J =1, conditional formatting sets the background to a hash (no response required) to indicated a not applicable maturity question.
J2	The value calculated with this formula counts the number of questions on the tab.
J ***<Q Depth>***	Values in this column indicate the depth (number of periods) the question has.
K ***<Table ID>***	A value of "1" in this cell indicate the top of a table.
L ***<1>***	This formula is used to calculate the first digit of the question number. It looks to see if there is a value in the cell above, if not it assumes the value should be a 1. Next it looks to see if the depth is 1, If so, it will increment by one, if not it pulls down the value from the cell above.
M - P ***<2 - 5>***	This formula is used to calculate the second through fifth digits of the question number. It first looks at the cell above and if blank it assumes a 0. If not blank, it looks at it's next highest neighbor above to see if there is a transition, it there is a transition then it resets to 0, Lastly it looks at the question depth to see if it is the same depth as above. If so it increments, if not it will pull down the value from above.
Q ***<HL Ans>***	This formula is used to carry over and convert the answer from the Lite tab to a number on the detail tabs. The VLOOKUP will search the L2_Array named field to find the question serial number and bring back the answer number in that array. For proper SMT operation, if a Master SIG is created then high level responses are ignored. **Note**: This function has been removed in the 2018 SIG. However, the L2 array still exists to ensure backward compatability.
R ***<Loc Ans>***	This formula converts the local answer to a number. It first checks to see if the depth is not blank. If it is then assumes the answer should be blank. If the depth field is not blank the formula converts the local answer to a number. 0 = No answer, 1 = "Yes", 2 = "No" and 3 = "N/A".
S ***<Comb Ans>***	This formula is used to combine the high level answer and the local answer. If the question depth is blank a blank is assumed. Responses are evaluated in the following order 1st - Lite, 2nd - local response.

T2	The value calculated with this formula counts the number of questions on the tab. This value is used by a formula on the Drops tab to calculate the total questions on the tab.
T ***<Table Calc (Tot Q#)>***	The value in this cell determines if the question is actually a question or if it is part of a response list for a question. The logic looks above, below and in column H to make the determination.
U ***<Q Carry Dn>***	This formula carries parent responses down to it's children. It first looks for a blank in the question depth and if blank will carry down the value from above. If the question has been answered it will bring over the question depth. If the questions not answered it will compare the local question depth to the previous value if the depth is greater the previous value will be carried down, if not it will turn to 0.
V ***<Resp Calc>***	This formula works with the Q Carry Dn formula to carry the value of the response down. If response is No or N/A those responses values are carried down to the next parent question. For proper SMT operation, if Master is selected (this tab, D6) response carry down is disabled.
W ***<T Carry Dn>***	The value in this cell identifies if a question in a table has been answered. If any value in a response list is answered the result will be rolled up the next cell until it reaches the list identifier.
X2	The formula in this cell counts the number of answered questions. This value is used by a formula on the Drops tab to calculate the total questions answered on the tab.
X ***<Final Ans>***	The result in this cell determines if a question has been answered and is used to count the actual questions answered not answers as part of a response list. This is a simple AND function to combine the values in columns T, S and V.
Y1	The formula in this cell calculates the total number of rows used on the tab.
Y **<Question Level>**	Used to identify the scoping level of the question: 1 = Filter 2 = Lite 3 = Core 4 = Full
Z **Category**	Identifies the category of the question
AA **Sub-Category**	Identifies the sub-category of the question
AB **Optional Scoring**	Provides a field for the user to provide their own value for the question. This field is only displayed when a Master SIG is created.
AC **<Automation Filter>**	This value is macro generated and determines if the question should be displayed or not when tab automation is endabled. The macro calculates if the question is a parent and what it's response is and will then add a 1 or 2 to identify displayed questions. It then applys an auto-filter to the column to hide the chidren.
AD **<Maturity N/A>**	Used to hash the maturity field. This field may be updated my the macro depending on the response. If the response is No or N/A this field gets updatd and the formatting removed from the maturity field.
AE **<Scoping Filter>**	The value in this field is macro generated and determines if the question should be displayed or not. If there is an x in the field the question will appear, if it's blank the question will be hidden by the auto-filter. This value is updated when the SIG is scoped.
AF **Question Level**	Shows the scoping level of the question (see Y <Question Level> above). This field is only displayed when a Master SIG is created.

Column (Cell)	Formula
A	Hard coded, unique serial number (Rows without questions have no serial numbers)
A4 (some tabs location is different)	MAX(An:An)
D Conditional Formatting	
E Conditional Formatting	
I	Manually entered question depth value (0 - 5)
J	Manually entered table top identifier (if 1 than table top)
K	IF(Kn-1="",1,IF(In=1,Kn-1+1,Kn-1))
L (M - O) are similar	IF(Ln-1="",0,IF(Kn-1<>Kn,0,IF($In=2,Ln-1+1,Ln-1)))
P	IF(OR(Master="Master",In=0,Jn=1),0,IF(ISNA(VLOOKUP(An,L2_Array,21,FALSE)),0,VLOOKUP(An,L2_Array,21,FALSE)))
Q	IF(In="","",IF(Dn="Yes",1,IF(Dn="No",2,IF(Dn="N/A",3,0))))
R	IF(In="","",IF(Pn>0,Pn,IF(Qn>0,Qn,0)))
S	IF(OR(In="",In=0),"",IF(OR(In=1,Sn-1=""),1,IF(OR(AND(Jn-1=1,(In-In-2<>0)),AND(Sn-1=0,In-1=I5),AND(Jn-1=1,In=In-2)),0,1)))
T	IF(In="",Tn-1,IF(AND(Rn>1,OR(Tn-1="",Tn-1=0,Tn-1>=In)),In,IF(In>Tn-1,Tn-1,0)))
U	IF(Master="Master",Qn,IF(Un-1="",Rn,IF(OR(AND(Tn>0,Rn<Un-1),AND(Tn=1,Rn<=Un-1)),Un-1,Rn)))
V	IF(In="","",IF(OR(AND(Sn-1=1,Tn=1),Rn>0,AND(Sn+1=0,Vn+1=1)),1,0))
W	IF(In="","",IF(OR(AND(Tn>0,Sn=1),AND(Sn=1,Vn=1)),1,0))
X	IF(ISNA(VLOOKUP(An,L2_Array,1,FALSE)),"",1)
Sheet Protection	QKsR3Uwg