



**Solicitation Information**  
**April 24, 2017**

**RFP# 7551585**

**TITLE: PROGRAM AND PROJECT MANAGEMENT SOFTWARE INTEGRATION**

**Submission Deadline: May 23, 2017 at 2:00 PM (ET)**

Questions concerning this solicitation must be received by the Division of Purchases at [gail.walsh@purchasing.ri.gov](mailto:gail.walsh@purchasing.ri.gov) no later than **Friday, May 5, 2017 at 5:00 PM (ET)**. Questions should be submitted in a *Microsoft Word attachment*. Please reference the RFP# on all correspondence. Questions received, if any, will be posted on the Internet as an addendum to this solicitation. It is the responsibility of all interested parties to download this information.

**SURETY REQUIRED: No**

**BOND REQUIRED: No**

GAIL WALSH  
CHIEF BUYER

Applicants must register on-line at the State Purchasing Website at [www.purchasing.ri.gov](http://www.purchasing.ri.gov)

**Note to Applicants:**

Offers received without the entire completed three-page RIVIP Generated Bidder Certification Form attached may result in disqualification.

**THIS PAGE IS NOT A BIDDER CERTIFICATION FORM**

**TABLE OF CONTENTS**

Section 1 –Introduction	3
Section 2- Background	5
Section 3- Scope of Work	5
Section 4 -Technical Proposal	9
Section 5 -Cost Proposal	9
Section 6- Proposal Submission	10
Section 7 –Evaluation and Selection	11

Attachment A - Detailed Technical Requirements  
Attachments B1, B2, B3, B4, and B5 – Sample URI project spreadsheets  
Attachments C1 and C2 – URI Security Requirements

## **SECTION 1: INTRODUCTION**

The Rhode Island Department of Administration/Division of Purchases, on behalf of the University of Rhode Island OFFICE OF CAPITAL PROJECTS, is soliciting proposals from qualified firms to provide PROGRAM AND PROJECT MANAGEMENT SOFTWARE INTEGRATION in accordance with the terms of this Request for Proposals and the State's General Conditions of Purchase, which may be obtained at the Rhode Island Division of Purchases Home Page by Internet at [www.purchasing.ri.gov](http://www.purchasing.ri.gov) .

This is a Request for Proposals, not an Invitation for Bid. Responses will be evaluated on the basis of the relative merits of the proposal, in addition to price; there will be no public opening and reading of responses received by the Division of Purchases pursuant to this Request, other than to name those offerors who have submitted proposals.

### **INSTRUCTIONS AND NOTIFICATIONS TO OFFERORS:**

1. Potential vendors are advised to review all sections of this RFP carefully and to follow instructions completely, as failure to make a complete submission as described elsewhere herein may result in rejection of the proposal.
2. Alternative approaches and/or methodologies to accomplish the desired or intended results of this procurement are solicited. However, proposals which depart from or materially alter the terms, requirements, or scope of work defined by this RFP will be rejected as being non-responsive.
3. All costs associated with developing or submitting a proposal in response to this RFP, or to provide oral or written clarification of its content shall be borne by the vendor. The State assumes no responsibility for these costs.
4. Proposals are considered to be irrevocable for a period of not less than 120 days following the opening date, and may not be withdrawn, except with the express written permission of the State Purchasing Agent.
5. All pricing submitted will be considered to be firm and fixed unless otherwise indicated herein.
6. Proposals misdirected to other state locations, or which are otherwise not present in the Division at the time of opening for any cause will be determined to be late and will not be considered. For the purposes of this requirement, the official time and date shall be that of the time clock in the reception area of the Division.

7. It is intended that an award pursuant to this RFP will be made to a prime vendor, or prime vendors in the various categories, who will assume responsibility for all aspects of the work. Joint venture and cooperative proposals will not be considered. Subcontracts are permitted, provided that their use is clearly indicated in the vendor's proposal and the subcontractor(s) to be used is identified in the proposal.
8. All proposals should include the vendor's FEIN or Social Security number as evidenced by a W9, downloadable from the Division's website at [www.purchasing.ri.gov](http://www.purchasing.ri.gov).
9. The purchase of services under an award made pursuant to this RFP will be contingent on the availability of funds.
10. Vendors are advised that all materials submitted to the State for consideration in response to this RFP will be considered to be Public Records as defined in Title 38, Chapter 2 of the General Laws of Rhode Island, without exception, and will be released for inspection immediately upon request once an award has been made.
11. Interested parties are instructed to peruse the Division of Purchases website on a regular basis, as additional information relating to this solicitation may be released in the form of an addendum to this RFP.
12. Equal Employment Opportunity (G.L. 1956 § 28-5.1-1, et seq.) – § 28-5.1-1 Declaration of policy – (a) Equal opportunity and affirmative action toward its achievement is the policy of all units of Rhode Island state government, including all public and quasi-public agencies, commissions, boards and authorities, and in the classified, unclassified, and non-classified services of state employment. This policy applies to all areas where State dollars are spent, in employment, public services, grants and financial assistance, and in state licensing and regulation. For further information, contact the Rhode Island Equal Opportunity Office at (401) 222-3090 or [krystal.waters@doa.ri.gov](mailto:krystal.waters@doa.ri.gov).
13. In accordance with Title 7, Chapter 1.2 of the General Laws of Rhode Island, no foreign corporation, a corporation without a Rhode Island business address, shall have the right to transact business in the State until it shall have procured a Certificate of Authority to do so from the Rhode Island Secretary of State (401-222-3040). *This is a requirement only of the successful vendor(s).*
14. The vendor should be aware of the State's Minority Business Enterprise (MBE) requirements, which address the State's goal of ten percent (10%) participation by MBE's in all State procurements. For further information, contact the MBE Administrator at (401) 574-8670 or [Dorinda.keene@doa.ri.gov](mailto:Dorinda.keene@doa.ri.gov). or visit the website [www.mbe.ri.gov](http://www.mbe.ri.gov).

15. The State reserves the right to award to one or more offerors. The State also reserves the right to award this project based on pricing alone.

## **SECTION 2: BACKGROUND**

### MISSION OF THE UNIVERSITY OF RHODE ISLAND

The University of Rhode Island (URI) is the State's public learner-centered research university. We are a community joined in a common quest for knowledge. The University is committed to enriching the lives of its students through its land, sea, and urban grant traditions. URI is the only public institution in Rhode Island offering undergraduate, graduate, and professional students the distinctive educational opportunities of a major research university. Our undergraduate, graduate, and professional education, research, and outreach serve Rhode Island and beyond. Students, faculty, staff, and alumni are united in one common purpose: to learn and lead together. Embracing Rhode Island's heritage of Independent thought, we value: **Creativity and Scholarship, Diversity, Fairness, and Respect, Engaged Learning and Civic Involvement, and Intellectual and Ethical Leadership**

### PROJECT BACKGROUND

The University of Rhode Island Offices of Campus Planning & Design and Capital Projects seek to consolidate our existing methods of project management tracking into a consolidated system that allows for our design teams, contractors, and University staff to interact and track project details on both an individual project and on a campus-wide (program) basis. The existing method of tracking major capital projects is achieved through a variety of project software programs that changes on a project-by-project basis depending on several factors. The University currently tracks individual project details through the use of several software programs and spreadsheets in combination with ad hoc reporting and interaction with our campus financial software. Our goal is to standardize our capital project management from starting with conceptual development, continuing throughout design, then bidding, construction and close out, and finally archiving the project details and delivery to our Facilities staff.

## **SECTION 3: SCOPE OF WORK**

### **General:**

Vendor will provide a full service program and project management software system for URI's Offices of Campus Planning & Design and Capital Projects. Vendor will analyze URI's existing work flow for capital project development and delivery and then integrate software into our current and projected capital project work program that utilizes modern technologies to consolidate and expedite work and reduce costs.

## **Minimum Technical Requirements:**

### Flexibility

Software must be able to be modified to reflect internal and external work processes. URI expects selected software to have out-of-the-box features that reflect standard practices in project and program management such as project estimating, multiple financial account capability, project scheduling integration, procurement and contract management, construction documentation management (requests for information, construction change directives, submittals, requisitions, etc.), etc. URI must be able to use this system internally for basic project and program management and we need all our design consultants and construction team (owner's project managers, contractors and subcontractors, etc.) to be able to access the system as needed for their unique role for specific projects. URI anticipates that URI will have the most robust use of the software while other users (consultants and contractors) will have limited access based on their roles in project management.

### Comprehensiveness

Software must be modified/integrated to reflect URI internal and external work flow processes and to reduce duplication of data entry wherever feasible. Data should be stored in a single and fully integrated database.

### Modularity

This initial engagement will have a limited integration of URI work flow processes that focus on construction and design project management and fiscal management. Future engagements could include (but not be limited to) full integration with legacy financial software (PeopleSoft), facilities management software (IBM Tririga), State of RI capital planning (Microsoft Access), AIA contract document software, etc. Software must be able to be improved through future integration efforts as need and funding permits.

### Ease-of-Use

Software must have a simple graphical user interface that is customized for two basic user groups:

**URI staff:** Includes Project Managers, Financial Managers, and Executive Management. URI staff will have access to approve and advance decisions based on their project management roles. URI staff interface must be refined for Project Managers (full access, "power users"), Financial Managers (access to budgetary, contract, and scheduling modules), and Executive Management (access to program-wide schedules, financial reports, project status reports, etc.).

**Design and Construction Teams:** Design team includes architects and engineers that upload plans, provide initial approval of submittals, RFI's, pay requisitions, etc. Construction team includes contractors and primary subcontractors that will upload pay requisitions, submittals, change order requests, etc. Generally all actions from the Design and Construction teams require a subsequent action and/or authorization from URI staff.

GUI must be easy to use and to access basic functions at a glance and be consistent with industry standards for process control and terminology.

## **Detailed Technical Requirements - Summary**

### Architecture

The proposed solution shall have an n-tier architecture that is fully capable of operating via web browsers on conventional PC's, iOS, and mobile platforms. The proposed solution shall be J2EE compliant. Software cannot utilize "web enabled" or "browser wrapper" solutions to achieve web based functionality.

### Interface to Existing Systems

Initial software integration must include the ability to interface to URI PeopleSoft Financials existing functionality, including reconciliation with accounts and vendors. Through the initial consultation with URI's IT staff, vendor will assess and propose an appropriate frequency for reconciliation (at least weekly).

URI uses Excel spreadsheets to manage project budgets. This integration will include mapping URI budget spreadsheets into project management software from project concept through design, and then into bidding and construction. Examples of URI's spreadsheets are **Attachments B1, B2, B3, B4, and B5**, attached for your information.

URI also uses spreadsheets to track contracts for design, contracted services, and goods. These "project budget spreadsheets" will be integrated into the project management software.

URI must seek authorization externally for procurement of goods and services and for use of certain funding sources. URI uses a combination of transmittal letters (Word documents), spreadsheets, and hand delivered and hand written checklists that are to be mapped to the external processes. Similarly URI receives authorization from external sources (via PDF documents) and must store this information along with other project documentation for future reference.

URI must be able to interface/upload project schedules in electronic format (Microsoft Project, Primavera, etc.) for use in both project scheduling and financial estimating (drawdown schedules).

### Import/Export Capabilities

Data compiled and developed through the software system must be able to get exported in the following formats: Excel spreadsheets (for financial data), Word documents (for regular forms that are sent externally for information or approval), PDF's (for scanned images, project records such as emails and other software), Microsoft Project (for project schedules), and Access (for database files).

### Software Security

Software will be used by both URI staff as well as external consultants and contractors. Software must provide appropriate controls so that users and/or user groups must be granted unique access to the system according to their role/login. Generally speaking URI staff user group will have approval rights on most project management functions. Consultants and Contractors are able to upload/download information and advance information for subsequent action by other user groups. The selected consultant will work with URI staff to map these work flows (following industry practices between consulting architects/engineers, contractors, and owners) and develop appropriate security that correlates to the user functions. All vendors proposing under this contract must fill out **Attachments C1 and C2** in its entirety.

### Administration Console

Software must have an administrative console for URI user group to assess technical and system information as it relates to the functionality of overall system. Required system information includes but shall not be limited to CPU utilization, available memory, build number, database and network connections.

### Detailed Technical Requirements (must answer all questions)

The charts in **Attachment A** must be filled out in order for your bid to be considered complete. From this point forward, mandatory requirements will include the word “shall.” For every requirement with “shall,” the proposed solution must comply. Proposals offering solutions that cannot meet any mandatory requirement will be set aside without further consideration.

### Integration and Implementation Schedule

The schedule for this project is as follows:

Integration: June 2017 – July 2017

Implementation: July 2017 – August 2017

### Budget

The Integration and Implementation budget for this program is estimated at \$120,000, inclusive of all consulting, licensing, software and hardware costs. This project will result in a fully functional software system for the upcoming fiscal year (beginning July 1, 2017 and ending June 30, 2018). Thereafter the software system is expected to have an annual maintenance expense that will accommodate the fluctuating number of design professionals, contactors, and URI employees that will need to access the integrated system. Vendors must specify what the annual costs for maintenance of the system are expected to be given approximately 20 internal URI users and up to 50 external (consultant and contractor) users at any one given point in time. It is understood that these estimates are not concurrent users and that the selected vendor must optimize their licensing proposal so as not to burden URI’s annual software maintenance costs.



## **SECTION 4: TECHNICAL PROPOSAL**

Narrative and format: The separate technical proposal should address specifically each of the required elements:

1. Executive Summary - The executive summary is intended to highlight the contents of the Technical Proposal and to provide evaluators with a broad understanding of the offeror's technical approach and ability;
2. Capability, Capacity and Qualifications of the Offeror - This section shall include identification of all staff and/or subcontractors proposed as members of the project team, and the duties, responsibilities and concentration of effort which apply to each (as well as resumes, curricula vitae or statements of prior experience and qualification). Please emphasize prior and ongoing work with university and college capital programs.
3. Work Plan/Approach Proposed - This section shall describe the offeror's understanding of the State/University's requirement, including the result(s) intended and desired, the approach shall discuss and justify the approach proposed to be taken for each task and the technical issues that will or maybe confronted at each stage on the project. The work plan description shall include a detailed proposed project schedule (by task and subtask), a list of tasks, activities, and/or milestones that will be employed to administer the project, the-assignment of staff members and concentration of effort for each, and the attributable deliverables, for each and will identify and describe what type of tutor training - methodology will be utilized in the program,
4. Previous Experience and Background, including a comprehensive listing of similar projects undertaken and/or similar clients served, including a brief description of the projects. Also include a description of the business background or the offeror (and all subcontractors proposed), including a description of their financial position.

## **SECTION 5: COST PROPOSAL**

A separate, signed and sealed, Cost Proposal reflecting the fee structure proposed for this project must be included in your submission. There are two components that must be included in your Cost Proposal. The first component is the Integration and Implementation in the following four phase work format:

- 1- **Initial Consultation and Workflow Mapping**
- 2- **Software Design and Integration**
- 3- **Staff Training and Field Testing**
- 4- **Software Deployment and Owner Acceptance**

The second component is the Annual Software License cost. This is the cost that URI will incur each year to maintain the software (as configured and accepted) each year, given the total number of internal and external users. This proposal will include the first year's licensing fees for the software to run from June 1, 2017 to June 30, 2018.

## **SECTION 6: PROPOSAL SUBMISSION**

Questions concerning this solicitation may be e-mailed to the Division of Purchases at [gail.walsh@purchasing.ri.gov](mailto:gail.walsh@purchasing.ri.gov) no later than the date and time indicated on page one of this solicitation. Please reference **RFP #7551585** on all correspondence. Questions should be submitted in a Microsoft Word attachment. Answers to questions received, if any, will be posted on the Internet as an addendum to this solicitation. It is the responsibility of all interested parties to download this information. If technical assistance is required to download, call the Help Desk at (401) 222-3766 or [lynda.moore@doit.ri.gov](mailto:lynda.moore@doit.ri.gov).

Offerors are encouraged to submit written questions to the Division of Purchases. **No other contact with State parties will be permitted.** Interested offerors may submit proposals to provide the services covered by this Request on or before the date and time listed on the cover page of this solicitation. Responses received after this date and time, as registered by the official time clock in the reception area of the Division of Purchases will not be considered.

Responses (**an original plus (6) copies**) should be mailed or hand-delivered in a sealed envelope marked "**RFP# 7551585 Program and Project Management Software Integration**" to:

RI Dept. of Administration  
Division of Purchases, 2nd floor  
One Capitol Hill  
Providence, RI 02908-5855

NOTE: Proposals received after the above-referenced due date and time will not be considered. Proposals misdirected to other State locations or those not presented to the Division of Purchases by the scheduled due date and time will be determined to be late and will not be considered. Proposals faxed, or emailed, to the Division of Purchases will not be considered. The official time clock is in the reception area of the Division of Purchases.

## RESPONSE CONTENTS

Responses shall include the following:

1. A completed and signed four-page R.I.V.I.P generated bidder certification cover sheet downloaded from the RI Division of Purchases Internet home page at [www.purchasing.ri.gov](http://www.purchasing.ri.gov).
2. A completed and signed W-9 downloaded from the RI Division of Purchases Internet home page at [www.purchasing.ri.gov](http://www.purchasing.ri.gov).
3. **A separate Technical Proposal** as outlined within section 4 including Executive Summary; Capability, Capacity, and Qualifications of the offeror; Work plan/approach proposed; Previous experience and background.
4. **A separate, signed and sealed Cost Proposal** reflecting the hourly rate, or other fee structure, proposed to complete all of the requirements of this project.
5. **The Standards Information Gathering (SIG) Questionnaire** will need to be completed by each vendor. The SIG is intended to simplify and speed up the process of gathering the information to assess the controls used by the vendor's organization to protect the University's data, comply with the terms of the agreement and to provide an operationally stable, protected and recoverable source. You may access this Questionnaire at: <https://security.uri.edu/forms/sig>

The printed SIG response must be included with your response and will be forwarded to and reviewed by the URI Associate Director of Information Security.

In addition to the multiple hard copies of proposals required, Respondents are requested to provide their proposal in **electronic format (CD-Rom, disc, or flash drive)**. Microsoft Word / Excel OR PDF format is preferable. Two electronic copies are requested (One for the State and one for the University) and it should be placed in the proposal marked "original".

## **SECTION 7: EVALUATION AND SELECTION**

Proposals will be reviewed by a Technical Review Committee comprised of staff from state agencies. To advance to the Cost Evaluation phase, the Technical Proposal must receive a minimum of 60 (85.7%) out of a maximum of 70 technical points. Any technical proposals scoring less than 60 points will not have the cost component opened and evaluated. The proposal will be dropped from further consideration.

Proposals scoring 60 technical points or higher will be evaluated for cost and assigned up to a maximum of 30 points in cost category, bringing the potential maximum score to 100 points.

The University of Rhode Island reserves the exclusive right to select the individual(s) or firm (vendor) that it deems to be in its best interest to accomplish the project as specified herein; and conversely, reserves the right not to fund any proposal(s).

Proposals will be reviewed and scored based upon the following criteria:

<b>Criteria</b>	<b>Possible Points</b>
Staff Qualifications	10 Points
Capability, Capacity, and Qualifications of the Offeror	20 Points
Quality of the Work plan	20 Points
Suitability of Approach/Methodology	20 Points
<b>Total Possible Technical Points</b>	<b>70 Points</b>
Cost calculated as lowest responsive cost proposal divided by (this cost proposal) times 30 points *	30 Points
<b>Total Possible Points</b>	<b>100 Points</b>

\*The Low bidder will receive one hundred percent (100%) of the available points for cost. All other bidders will be awarded cost points based upon the following formula:

$(\text{low bid} / \text{vendors bid}) * \text{available points}$

For example: If the low bidder (Vendor A) bids \$65,000 and Vendor B bids \$100,000 and the total points available are Thirty (30), vendor B's cost points are calculated:  $\$65,000 / \$100,000 * 30 = 19.5$

Points will be assigned based on the offeror's clear demonstration of his/her abilities to complete the work, apply appropriate methods to complete the work, create innovative solutions and quality of past performance in similar projects.

Applicants may be required to submit additional written information or be asked to make an oral presentation before the technical review committee to clarify statements made in their proposal.

## **CONCLUDING STATEMENTS**

Notwithstanding the above, the State reserves the right not to award this contract or to award on the basis of cost alone, to accept or reject any or all proposals, and to award in its best interest.

Proposals found to be technically or substantially non-responsive at any point in the evaluation process will be rejected and not considered further.

The State may, at its sole option, elect to require presentation(s) by offerors clearly in consideration for award.

The State's General Conditions of Purchase contain the specific contract terms, stipulations and affirmations to be utilized for the contract awarded to the RFP. The State's General Conditions of Purchases/General Terms and Conditions can be found at the following URL: <https://www.purchasing.ri.gov/RIVIP/publicdocuments/ATTA.pdf>

- End -

RFP # 7551585

**PROGRAM AND PROJECT MANAGEMENT SOFTWARE INTEGRATION**

**Attachment A – Detailed Technical Requirements (must answer all questions)**

The following charts must be filled out in order for your bid to be considered complete. From this point forward, mandatory requirements will include the word “shall.” For every requirement with “shall,” the proposed solution must comply. Proposals offering solutions that cannot meet any mandatory requirement will be set aside without further consideration.

In the following tables vendors are also instructed to indicate one of the following for each requirement.

- Yes                      Current version of the proposed solution meets the said requirement with no modifications.
- Yes w/Mod            Current version of the proposed software will meet the said requirement with modification (“Mod”). When indicating “Yes w/Mod,” vendors must describe the extent of customizations that are required in either the “Vendor Comments” column or on additional pages. Failure to do so will result in disqualification.
- No                        Proposed solution cannot meet the said requirement.

A number of requirements will instruct vendors to provide an explanation of how the proposed system meets the said requirement. Use the “Vendor Comments” column to provide explanations, notes, or cross references to additional pages. Lengthy explanations may be submitted as attachments. Failure to answer any requirement will result in disqualification.

Document Management Requirements					
Item #	Requirement	Yes	Yes w/ Mod.	No	Vendor Comments
1.	The proposed solution shall include Document Management capabilities. Provide an overall description of the system’s Document Management applications.				

2.	The Document Management application shall allow users to post documents (e.g., Word Documents, Excel Spreadsheets, emails, PDF files) to a central repository.				
3.	It should be easy to upload/download multiple documents directly to a record instead of first uploading them to the database and then to the record. Ideally, users will select files to an applet window and hit upload or download - or simply drag them over to the upload/download window.				
4.	It shall be possible to download whole folder structures from the proposed solution to a computer.				
5.	The Document Management system shall include revision and versioning control to maintain document integrity. Describe how the proposed solution meets this requirement.				
6.	There shall be discussion threads associated with each record in the system so users can share comments.				
7.	Describe the system's search and filtering capabilities.				



8.	The Document Management application shall include redlining capabilities.				
9.	Application shall support user defined document hierarchies by company and projects.				
10.	Release control and check-in/check-out services. Services shall secure document while in use and prevent updates by others until document is made available.				
11.	Application shall provide the ability to collaborate with external vendors / architects / engineers on design and specification documents, including the ability to view and redline.				
12.	Application shall support revision and version control on all document types.				
13.	Application shall provide ability to associate document(s) with specific project work steps.				
14.	Describe how security settings can be employed to help ensure document integrity.				

Cost Code Management					
#	Requirement	Yes	Yes w/ Mod.	No	Vendor Comments

15.	Application shall provide a summary of all costs related to a project including initial pro forma budgeting, specific funding source commitments, incurred costs and forecasts.				
16.	All changes related to costs should be tracked by an Audit Trail Including Approval fields.				
17.	Service Code reference fields should be tailored to meet URI's requirements.				
18.	Retired Project Costs should be available for viewing and comparison to current Project Costs.				
19.	All Financial transactions must require reviewer and approval information.				

Proposal Management					
#	Requirement	Yes	Yes w/ Mod.	No	Vendor Comments
20.	Application must upload and store bid package and advertisement. These are external processes that must be mapped with URI and State Purchasing staff.				
21.	Application must upload and store all vendor inquires, addenda, and other pre bid documentation.				

22.	Application must upload and store all post bid qualification submissions including insurance certificates, bonding, and other documentation as required by the bid documents.				
-----	---	--	--	--	--

Procurement Management					
#	Requirement	Yes	Yes w/ Mod.	No	Vendor Comments
23.	Capability to interface with URI PeopleSoft Financials existing functionality				

Contract Management					
#	Requirement	Yes	Yes w/ Mod.	No	Vendor Comments
24.	The proposed solution shall centrally store and track all contract documentation and information, including associated assets, critical dates and actions, financial transactions, options, conditions, and clauses.				

25.	<p>Out of box, the proposed Contract Management module shall track the following types of contracts:</p> <ul style="list-style-type: none"> <li>• Blanket Order</li> <li>• Purchase Order</li> <li>• Purchase Requisition</li> <li>• Service Agreement</li> <li>• Standard Contract</li> <li>• Warranty</li> </ul>				
26.	<p>A Service Agreement is created when a contract exists between a vendor and a project for the vendor to supply materials and/or services at a specified price within a specified time period.</p> <p>The Service Agreement Record must describe the specific details of pricing and lead times for products, and hourly rates for services, in addition to other detailed information about products and services. Describe how the proposed solution meets this requirement.</p>				
27.	<p>The application must track asset and equipment warranties with alerts for warranties due to expire.</p>				

28.	Contracts must contain fields to define cost breakdown for measurement and Payment.				
29.	Managing the execution and development Schedule of contracts is critical to URI, fields must include planned start, end and duration as well as actual start end and duration.				

Payment Management					
#	Requirement	Yes	Yes w/ Mod.	No	Vendor Comments
30.	Capability to interface with URI PeopleSoft Financials existing functionality.				

Reporting Requirements					
Item #	Requirement	Yes	Yes w/ Mod.	No	Vendor Comments
31.	Describe the proposed system's overall design and approach to creating reports.				
32.	What is the learning curve for end users to customize reports within your product? What skill set does the end user need?				
33.	Is your product strictly a reporting tool? If not, please explain what other features it has.				
34.	Users shall be able to "drill down" into graphical reports and change the type of graph (e.g., pie, bar graph).				
35.	The proposed solution shall include a number of standard or "canned" reports. In the comments column, please describe how many standard reports are available.				
36.	Reports shall be easily exported to Excel and other formats supported by business intelligence.				

37.	Can your product host data from multiple application sources such as Asset Suite, eSOMS, P6, PeopleSoft, Excel, Access db etc? How difficult is it to add a new data source at a later time?				
38.	Reports shall be routed to any networked printer.				

General Project Management Requirements					
Item #	Requirement	Yes	Yes w/ Mod.	No	Vendor Comments
39.	The proposed system shall feature a rich project management functionality including setup and management of multiple project types and delivery methods, budget management, schedule management including Gantt chart scheduling, project contact management, issues and risk management, vendor and contractor management, bids and proposal management, procurement management, meeting management, document management and punchlist and closeout management. The system should feature flexible form design and data requirements, configurable business process workflow, and flexible online and printed reporting capabilities.				
40.	For ease of use, the application shall offer a dashboard that is completely flexible to layout and may be configured by role, geography, business unit, etc.				



41.	For ease of use, the application shall offer the use of multiple proxy users. For example, if a Project Manager is on vacation, one—or more—alternate users can take action on his/her behalf.				
42.	In order to capture key project metrics, critical issues, cost and schedule variances across projects by hierarchy, the “dashboard” shall offer placement of on demand graphical reporting that consist of bar charts, pie charts, line graphs, etc. with full drill down into supporting information. All charts/reports should be exportable to outside applications such as Microsoft Excel™, Microsoft Word™ an Adobe Acrobat™.				
43.	Dashboard reports should offer full drill down into supporting documentation.				
44.	Application shall support a reporting engine that allows for scheduling of regularly run Executive and Project Status reports. These reports should be delivered either online or by e-mail to selected users at defined intervals.				

45.	Application shall offer configurable alerts for critical notifications that may be, but not limited to, critical issues, potential budget or schedule overruns, change management, etc. Alerts shall be sent to e-mail, flagged upon log in of next session, and on a portal in real time.				
46.	To eliminate redundant data entry and to leverage best practices, the application shall allow users to create unlimited templates for quick generation of projects, budgets, schedules, contracts, etc. Templates shall offer complete configuration of data fields, drop-down lists, search screens/views, workflows, etc.				
47.	To help users quickly find a project record, there shall be a search mechanism with user-configurable filter elements such as project type, manager, location, organization, name, etc. Please describe this feature.				
48.	For repetitive projects that are similar in scope, the application should offer complete project copy functionality based on user access and other security restrictions.				

49.	Application shall offer complete version and audit control to understand who, when, and why actions were taken or data changes were made.				
50.	Application shall support data importing of historical project and other data and for leveraging against future cost estimates				
51.	System should also permit a one-to-many project to work order relationship.				
52.	System shall support capabilities for vendor interaction /collaboration via a web browser.				
53.	Application shall allow addition of customized fields within records with no restriction to how many and placement.				
54.	Ability to configure workflow to support project management related processes (change management, bid process, contact/vendor management, etc.) shall be provided.				
55.	The project manager or other authorized individual shall have the ability to grant or deny access to specific users or user groups.				

56.	There shall be a mechanism to export data to Microsoft Word™, Microsoft Excel™, Adobe Acrobat™ and business intelligence reporting. Please describe this mechanism.				
-----	---	--	--	--	--

Budget Management					
Item #	Requirement	Yes	Yes w/ Mod.	No	Vendor Comments
57.	Application shall support a master budget code structure that can be copied into programs and projects.				
58.	Application shall support configurable budget code structures (URI uses the terminology “chart field strings”) without limitations to number of levels.				
59.	Application shall support multiple budget templates for various project types (e.g. new construction, existing construction, renovations, relocation, minor repairs classified as projects, closures, etc)				
60.	Budget codes shall support configurable fields within each area of budget management (Budgets, Commitments, Actuals, Forecast, etc).				

61.	Application shall support mapping of alternate coding structures to the master code structure.				
62.	Allow budget entry at the "line item" detail level or the "scope" (major) category level depending on the business process.				
63.	Ability to add comments/notes to the budget at the project, scope, and line item level.				
64.	Application shall support the ability to lock a budget upon approval and require approval for client specified transfers or changes.				
65.	Application shall support the ability to view all transactions against an individual budget code.				
66.	Application shall Alert a user (or set of users) when a budgeted amount exceeds a predetermined threshold based on business rules				
67.	All financial transactions shall automatically update the appropriate budget columns.				
68.	Application shall support full drill down from the budget into multiple levels of transactional data and decision process.				

69.	Ability to rollup and report budgets at any budget level (e.g. look at only general contractor costs).				
70.	System should provide ability to track and manage projected costs, pending costs and actuals including any authorized change orders or other budget changes.				
71.	Application shall provide visibility to and reporting of actual cost variances to budget at the line item, category, or total budget level.				
72.	Application shall support entering of notes for budget code forecasts to track reasons for adjustments				
73.	Application shall support tracking of historical cost averages and other consolidated financial transaction reporting				
74.	Application shall support multiple budget views and analysis (e.g. by project manager, program, project type company, geography, etc.)				

Project Scheduling					
Item #	Requirement	Yes	Yes w/ Mod.	No	Vendor Comments
75.	The ability to leverage and import schedule templates based on project types. Templates shall support the ability to have a predefined set of milestones, tasks, project teams, and responsibilities for each new project and/or program. Additionally, application shall support full flexibility to create, modify, and delete fields within project templates based on security access.				
76.	Application shall support the ability to manage multiple projects with different timelines and work breakdowns (e.g.: New Construction, Remodels, Dispositions, etc.).				
77.	Application should support multiple views of project schedule with visibility into task dependencies. (Gantt, Tasks, Project Status).				
78.	The system shall allow users to create and edit tasks through the Gantt chart, as well as within the task record.				
79.	Application shall provide the ability to integrate with Microsoft Project and other external scheduling applications.				

80.	System should provide ability to automatically assign or notify pre-defined assignees when a preceding task is completed. System should track the status of tasks and optionally provide email notifications when a task or milestone is completed.				
81.	Application shall provide the ability to add, monitor and report on comments as they relate to specific tasks.				
82.	System should provide ability to define and visually display each milestone date as mandatory or non-mandatory.				
83.	System shall provide the ability to send and receive notification for changed, upcoming, past-due milestones.				
84.	Application should provide ability to save a baseline for a project.				
85.	Application should provide report baseline vs. actual project schedule.				
86.	System should provide ability to maintain and view the historical record of all changes/revisions to the project schedule (with audit ID and timestamp).				



87.	Application shall provide flexibility to create custom, user defined forms attached to project tasks.				
-----	---	--	--	--	--

Project Contracts and Invoices					
Item #	Requirement	Yes	Yes w/ Mod.	No	Vendor Comments
88.	Application shall offer flexibility to generate a contract record manually or automatically populate a contract record from a bid award package.				
89.	Application shall offer flexibility to allow system-generated or custom contract number to the contract record.				
90.	Ability to select contract type (prime contract, subcontract, professional services, etc.) shall be provided.				
91.	Ability to select lump sum, unit price contract, or other contract terms shall be provided.				
92.	The application shall provide the ability to identify completion dates for substantial and final completion.				
93.	Ability to identify multiple milestone dates shall be provided.				
94.	Application shall provide the ability to track approval dates for contract execution.				

95.	Provide the ability to create a list of unit price items.				
96.	Ability to create a list of inclusions and exclusions shall be provided.				
97.	Workflow shall be flexible for approval routing to one or many delegates.				
98.	Ability to automatically update contract log shall be supported.				
99.	Ability to automatically update financial columns within budget shall be supported.				
100.	Ability to view change orders from the contract record shall be provided.				
101.	Ability to open change orders for edit directly from the contract record shall be provided.				
102.	Application shall provide the ability to create a contract invoice record.				
103.	Automatically imports contract line items into contract invoice record.				
104.	Application shall automatically update financial columns when new contract invoice is created.				
105.	Allows partial retainage and full release per line item.				
106.	Application shall show current status of contract billing.				

107.	Application shall allow linking of change orders to contract invoice and updates contract line items with Change Order details.				
108.	System should maintain records of payments and receipts to external entities such as third party vendors.				

Change Management					
Item #	Requirement	Yes	Yes w/ Mod.	No	Vendor Comments
109.	System shall provide the ability to create and track Change Orders from request to approval. Once approved does it must update commitments for the project,				
110.	System shall track issues and changes that arise through the lifecycle of the project, the resolutions to those problems, communication between individuals working on the issues, and the potential changes to the project from the original project plan stemming from those issues and resolutions.				
111.	Application shall provide the ability to create and manage potential change orders.				
112.	Can users manage multiple potential change orders and link them to a single event?				

113.	Can potential change orders link to the initiating document (RFI, drawing, correspondence, etc.)?				
114.	Does the system provide the ability to create a change order directly from a potential change order?				
115.	Does the system allow the creation of a change order without a potential change order, cost event, or quotation?				
116.	Can a change order support multiple line item changes as well as add additional items?				
117.	Can the system provide the ability to link design documents, including drawings and specifications, to change orders and potential change orders?				
118.	Does the system provide for the formalization of changes to contract completion dates through the execution of a change order?				
119.	Application shall provide the ability to create multiple line items within the potential change order record for multiple trades impacted.				
120.	Ability to assign each line item in the potential change order record as a budget impact, cost impact, or both budget and cost impact shall be provided.				

121.	Ability to assign potential change order line items to contractor impacted with Request For Proposal (RFP) shall be provided.				
122.	Application shall provide the ability to produce RFP document from potential change order record				
123.	Application shall provide the ability to link potential change order record to external supporting documents.				
124.	Change order record shall indicate original contract value and reflect changes in value.				
125.	Change order record shall indicate original completion dates and reflect changes to dates.				
126.	Application shall provide ability to link change order items to contract invoice record.				
127.	Application shall allow addition of customized fields within each area of Change Management				
128.	Ability to create customized workflow for Change Management process shall be provided.				
129.	Application shall provide ability for online approval of documents such as change orders, etc.				
130.	Does the system provide creation and tracking of Design Change Notices?				

Project Administration					
Item #	Requirement	Yes	Yes w/ Mod.	No	Vendor Comments
131.	Application shall provide ability to create Request for Information (RFI) record.				
132.	Ability to identify and route to online collaboration reviewers.				
133.	Ability to track dates for RFI review and answer shall be provided.				
134.	Application shall provide ability to identify if RFI is a potential cost impact.				
135.	Application shall provide ability to identify if RFI is a potential schedule impact.				
136.	Application shall provide ability to identify if RFI is a potential drawing (design) impact.				
137.	Ability to notify collaboration reviewers via Email or fax of RFI record.				
138.	Application shall provide ability to link electronic file of scanned document (sketch, memo, etc) to the RFI record and store within the database for viewing and printing.				
139.	Ability to create meeting minute record shall be provided.				

140.	Application shall provide ability to create multiple meeting minute sets for various meeting types.				
141.	Ability to link attendees from master vendor list to meeting minute record shall be provided.				
142.	Provides ability to identify attendee as present or absent.				
143.	Application shall provide ability to group meeting minute items by topic.				
144.	Ability to assign responsible party to meeting minute item shall be provided.				
145.	Application shall provide ability to assign status to each meeting minute item.				
146.	Application shall provide ability to track dates for each meeting minute item.				
147.	Ability to identify meeting minute item as Open/Closed.				
148.	Ability to generate meeting minute document from meeting minute record.				
149.	Application shall provide ability to create sequential meeting minute record and carry forward open items.				

150.	Application shall provide ability to link electronic file of scanned document (sketch, memo, etc) to the meeting minute record and store within the database for viewing and printing.				
151.	Ability to create submittal record shall be provided.				
152.	Application shall provide ability to link buyout item record to submittal record and populate basic data.				
153.	Ability to track dates for submittal processing and approval shall be provided.				
154.	Ability to track dates for submittal item scheduled delivery and actual delivery shall be provided.				
155.	Application shall provide ability to link submittal records to a submittal package record.				
156.	Application shall provide ability to link responsible company from master vendor list to submittal package record.				
157.	Ability to track review process of individual submittal items via a submittal package shall be provided				



158.	Application shall provide ability to link reviewer from master vendor list to the submittal package record.				
159.	Application shall provide ability to track dates for review process on a per register item basis.				
160.	Ability to identify reviewer action on a per item basis shall be provided.				
161.	Provide the ability to create a submittal package revision and link forward applicable data.				
162.	Application shall provide the ability to create product submittal document from submittal transmittal record.				
163.	Application shall create and track submittals and generate a submittals log.				
164.	Application shall provide ability to link recipient contact and company from master vendor list to transmittal records.				
165.	Application shall provide ability to link courtesy copy recipients from master vendor list to transmittal record.				
166.	Ability to identify and track receipt acknowledgement if required.				

167.	Application shall provide ability to link electronic file of scanned document (sketch, memo, etc) to the transmittal record and store within the database for viewing and printing.				
------	---	--	--	--	--

Field Management					
Item #	Requirement	Yes	Yes w/ Mod.	No	Vendor Comments
168.	The proposed system shall support and track the issuance of field instructions.				
169.	Can the proposed solution support and track the requirements for permits, the creation of permit applications, and the receipt of the issued permit?				
170.	Can the system support request and approval of project changes in a project defined format?				
171.	Does the system provide the ability to notify individuals or groups that are out of compliance with requirements set forth in the contract?				
172.	Does the solution support the management of accident reports?				
173.	Does the system support the distribution of safety notices of a project?				

174.	The system shall support the tracking of daily events pertaining to the project.				
175.	Does the system support the management of inspection and inspection requirements?				
176.	Does the system provide punch-list functionality with the ability to assign specific items to a project team member?				
177.	Ability shall be provided to create daily report record.				
178.	The proposed solution should track daily information on weather conditions.				
179.	Application shall provide ability to list all contractors on-site with work performed and crew size.				
180.	Application shall support ability to create notice to comply record directly from daily report record.				
181.	Application shall support ability to create safety notice record directly from daily report record.				
182.	Application shall provide ability to generate daily report document from daily report record.				

183.	Application shall provide ability to link electronic file of scanned document (sketch, memo, etc) can to the daily report record and store within the database for viewing and printing.				
------	--	--	--	--	--

Project Closeout					
Item #	Requirement	Yes	Yes w/ Mod.	No	Vendor Comments
184.	Application shall provide ability to create punchlists or closeout item records.				
185.	Report status of project tasks that shall be completed prior to closing the project (e.g. receipt of "as-built" information, completion of punch list) and pull the materials into a package so user doesn't have to search for the items in multiple places.				
186.	System should provide ability to track items on a project closeout checklist including: maintenance manuals, as-built drawings, punch lists, warranty information, etc.				
187.	Application shall track received and accepted dates for each closeout item record.				
188.	Generate closeout requirement document directly from the closeout item record.				

189.	Ability to create closeout record shall be provided.				
190.	Application shall provide ability to link electronic file of scanned document (sketch, memo, etc) to the closeout item or group record and store within the database for viewing and printing.				
191.	Does the system provide the ability to set a project to “inactive” status at close out, and restrict general access where users with permissions can only view project records and files while no further editing can be performed?				

Mobility					
Item #	Requirement	Yes	Yes w/ Mod.	No	Vendor Comments
192.	Does your system have mobile capabilities?				
193.	Please explain what the user can accomplish via mobile device.				
194.	Does your system have off-line capabilities?				
195.	How is the data entered off-line synchronized back into the application?				
196.	Is there an audit trail associated with the mobile process?				
197.	How do you ensure security during the transfer of information from off-line to the application?				

Performance Management					
Item #	Requirement	Yes	Yes w/ Mod.	No	Vendor Comments
198.	Does your company provide a Performance Management application?				
199.	Does the system include pre-defined performance indicators?				
200.	Are the performance management indicators integrated throughout the application?				
201.	Please list the key areas the performance management application targets.				
202.	Are standard reports included? Does the application provide customized reporting?				
203.	Is minimum and maximum metric targets/thresholds custom definable for interim and end-state goals?				
204.	Ideally there should be separate performance management portals for each application.				



**Consultant POs Consolidated Spreadsheet**  
**Multi Vendor**

	PO Amount	Amount Paid	Balance
\$	9,105,298.36	\$ 7,245,276.86	1,860,021.50

Project	PO#	Inv # or AOC	C.R. #	Date Rec'd	Date Paid	Accoun	CFS	OCP ID	PM	PO Amount	Amount Paid	Balance
210 Flagg - Room 211	43909	AOC	101428	05/24/16		9656	430-0000-0000-AP			(320.00)		(320.00)
210 Flagg - Room 211	43909	AOC	31643	08/31/12		9656	430-0000-0000-AP		RC	320.00		320.00
210 Flagg Road Floor Investigation	52332	10		10/20/15	11/02/15	9656	430-0000-0000-AP				1,500.00	(1,500.00)
210 Flagg Road Floor Investigation	52332	AOC	89743	07/01/16		9656	430-0000-0000-AP		RS	1,500.00		1,500.00
70 Lower College Rd Fire Escape	52332	1		06/07/13	06/28/13	9656	430-0000-0000-AP				3,500.00	(3,500.00)
70 Lower College Rd Fire Escape	52332	Unallocated Funds		01/14/13		9656	430-0000-0000-AP			3,500.00		3,500.00
Relocation Services for Fine Arts Music Library	107866	AOC	106420			9655	430-0000-0000-AP			5,815.00		5,815.00
Move HUB A/V Offices from Swan to Ranger Hall	107866	AOC	105971			9655	430-0000-0000-AP			1,275.00		1,275.00
Active Learning Classroom	43909	13		01/06/15	01/26/15	9656	100-4046-1212	KC.G.MISC.2013.002			1,405.00	(1,405.00)
Active Learning Classroom	43909	14		03/12/15	04/13/15	9656	100-4046-1212	KC.G.MISC.2013.002			100.00	(100.00)
Active Learning Classroom	43909	AOC	73865	11/14/14		9656	100-4046-1212	KC.G.MISC.2013.002	RC	1,505.00		1,505.00
Adams Hall Shower	43916	1		08/30/12	09/28/12	9656	210-5200-0000				1,600.00	(1,600.00)
Adams Hall Shower	43916	2		10/10/12	11/09/12	9656	210-5200-0000				500.00	(500.00)
Adams Hall Shower	43916	AOC	31761			9656	210-5200-0000		PD	2,100.00		2,100.00
Adams House	52332	1		06/07/13	06/28/13	9656	430-0000-0000-AP				4,000.00	(4,000.00)
Adams House	43909	2		11/27/12	12/21/12	9656	430-0000-0000-AP				480.00	(480.00)
Adams House	43909	AOC	31643	08/31/12		9656	430-0000-0000-AP		RC	480.00		480.00
Adams House	52332	Unallocated Funds		01/14/13		9656	430-0000-0000-AP		RS	4,000.00		4,000.00
Adams House - Structural Report	43909	2		11/27/12	12/21/12	9656	430-0000-0000-AP				360.00	(360.00)
Adams House - Structural Report	43909	3		02/01/13	03/08/13	9656	430-0000-0000-AP				2,200.00	(2,200.00)
Adams House - Structural Report	43909	AOC	31643	08/31/12		9656	430-0000-0000-AP		RC	2,560.00		2,560.00
Adams/Tucker/Fogarty/Washburn Study	43909	16		07/01/16	06/29/15	9656	100-4046-1212-P0000033				360.00	(360.00)
Adams/Tucker/Fogarty/Washburn Study	43909	17		07/01/16	07/03/15	9656	100-4046-1212-P0000033				9,690.00	(9,690.00)
Adams/Tucker/Fogarty/Washburn Study	43909	AOC	81289			9656	100-4046-1212-P0000033		RC	10,050.00		10,050.00
Additional CA Groups 2, 3, and 4	67975	AOC	46217	12/20/13		9656	446-0000-0000-P000027			39,080.00		39,080.00
Additional CA Groups 2, 3, and 4	67975	6		08/15/14	09/08/14	9656	446-0000-0000-P000027				16,155.00	(16,155.00)
Additional CA Groups 2, 3, and 4	67975	7		09/22/14	11/10/14	9656	446-0000-0000-P000027				8,697.50	(8,697.50)
Additional CA Groups 2, 3, and 4	67975	8		10/28/14	11/17/14	9656	446-0000-0000-P000027				11,250.00	(11,250.00)
Additional CA Groups 2, 3, and 4	67975	9		11/26/14	12/22/14	9656	446-0000-0000-P000027				2,977.50	(2,977.50)
Additional CA Groups 2, 3, and 4 - JH and BTG	67975	AOC	82507			9656	446-0000-0000-P000027			37,990.00		37,990.00
Additional CA Groups 2, 3, and 4 - JH and BTG	67975	16		06/23/15	08/11/15	9656	446-0000-0000-P000027				37,990.00	(37,990.00)
Aldrich and Burnside Entrances	43916	22		05/29/14	06/23/14	9656	210-5200-0000				5,000.00	(5,000.00)
Aldrich and Burnside Entrances	43916	23		06/11/14	06/30/14	9656	210-5200-0000				2,000.00	(2,000.00)
Aldrich and Burnside Entrances	43916	24		06/11/14	06/30/14	9656	210-5200-0000				1,000.00	(1,000.00)
Aldrich and Burnside Entrances	43916	AOC				9656	210-5200-0000		PD	68,000.00		68,000.00
Aldrich and Burnside Entrances	43916	Transfer	86520			9656	210-5200-0000			(60,000.00)		(60,000.00)
Allowance for Reimbursable Expenses	67975	AOC	46217	12/20/13		9656	446-0000-0000-P000027			2,221.80		2,221.80
Allowance for Reimbursable Expenses	67975	transfer				9656	446-0000-0000-P000027			(550.00)		(550.00)

↳ another tabs w/ links to vendors





**College Requisition Initial Processing Request Sheet**

PROJECT MANAGERS: Please initiate this College Requisition Processing Sheet which is the next step in Bidding, Advice of Change, Change in Account, MPAs. In order to do this you must provide the following complete information to the Business Office.

TO:	<b>OCP Business Office</b>
FROM:	Kenneth Burke
DATE:	8/5/2016
VENDOR ~ OR ~ BID LIST:	Ramtel
PURCHASE ORDER #:	107866
PROJECT NO.:	KC.G.RANG.2007.001

Assigned by P. Scott via PM

New Project Title: ~ OR ~	Ranger Hall - Harrington School Renovations
AOC/CR Description:	This CR is to purchase the Ramtel phones for the new Harrington School of Communication and Media for installation in each hallway. These are proprietary phones requested by the URI Public Safety Office. There is a blanket purchase order for these phones, and the installation of the phones has already been authorized to EW Burman under an earlier requisition.

Activity of Project:	<input type="checkbox"/> Architect/Engineer (9656)	<input type="checkbox"/> Fees ( Fire, Bldg Permit, etc.)
Please Check	<input type="checkbox"/> Site Improvements	<input type="checkbox"/> Bond Issuance Cost
(X) One Box	<input checked="" type="checkbox"/> Construction (9655)	<input type="checkbox"/> Other (Land Purchase, etc.)
	<input type="checkbox"/> Furniture/Equipment	

Proposal Cost:

Funding Source(s):	CHART FIELD STRING & PRICE	CHART FIELD STRING & PRICE
	9655-430-0000-0000 \$2,570.00	\$
		\$
		\$

New Projects: In accordance with plans & specs prepared by:

Fill In and dated:

Plans & Specs:

Check (X) One Box  Will be delivered  Have been delivered

Check (X) One Box  to RIBCC  to URI Purchasing

PO Close Date:  Typically one year after substantial completion or at end of warranty period and longer.

Purchases uses this date and will close the PO sometimes before final payment has been satisfied. Safe to go out 1.5 years.

**ATTACHMENTS REQUIRED:**

**NEW BIDS:**

PROJECT BUDGET - Updated from PM

BCC APPROVAL LETTER (if new bid)

4 CD's - (if new bid) STATE or LOCAL BID:  
 \* Invitation to Bid in Word  
 \* Bid Form in Word  
 \* Plans in one separate PDF  
 \* Specs in one separate PDF

SERF - ARRA JOBS ONLY

**AOC'S:**

PROJECT BUDGET - Updated from PM

PROPOSAL

MEMO - To justify and explain

Required on all:  Project Budget (Next Excel Tab)

**University of Rhode Island**

<b>Project Name:</b>	Ranger Hall - Harrington School Renovations
<b>Project Number:</b>	KC.G.RANG.2007.001
<b>Project Manager:</b>	Kenneth Burke
<b>DATE:</b>	8/5/2016

(from Liisa)

SOURCES	\$ AMOUNT	Cash Flow		
		FY2010 >>>>>>>	Through FY2011 \$ AMOUNT	FY2012
CFS Funding Goes Here	\$ -		\$ -	

EXPENSES	Unit cost	Estimate	Comments	Cash Flow		
				FY2010	FY2011	FY2012
<b>1. General Construction Costs</b>						
Demolition						
New Construction	/SF					
Renovation						
Roof Repair Allowance						
additional scope						
Design Contingency						
Skylight repair Contingency						
Construction Contingency						
		\$0	= #VALUE! /SF		\$ -	\$ -
<b>2. Site Preparation - Demolition and Landscaping</b>						
Building Demolition	LS	0				
Temporary Construction/Rel	LS	0				
On-site utilities	0.00%	0				
Hardscape	0.0%	0				
Landscaping	0.0%	0				
Construction Contingency	5.0%	0				
			Sum const = \$0			
<b>3. Building Design Fees and Testing Services</b>						
Programming	0.00%	0	incl. below			
Geotechnical [	0.0%	0				
Basic Fee		0				
Additional Con	#DIV/0!	0				
Additional Sen	#DIV/0!	0				
As-Builts		0				
Reimbursable		0				
Fees & Services Contingenc	5.0%	0				
TOTAL:		\$0			#VALUE!	#VALUE!
<b>4. Site Development Contribution - Non Site Specific</b>						
Utilities ( water, gas, storm,	LS	0				
Electrical Substation contrib	LS	0				
Utilities Engineering	LS	0				
Campus Master Planning cc	0.25%	0				
			Sum Site Developm ent = \$0		#VALUE!	#VALUE!
<b>5. Equipment &amp; Furnishings</b>						
Telephone/Data equipment	LS	0	from NETS			
Security systems	LS	0	from S&RM			
Furniture & Fixtures	\$0 SF	0				
Other Equipment (N.I.C.)	LS	0				
<b>6. Legal/Administrative Costs</b>						
Building Commissioning	LS	0 Est.				
Building Permit	0.3%	0 Est.				
Fire Marshall review	fee	0				
Liability Insurance	0.0%	0				
Builder's Risk insurance	0.1%	0				
Project Management		0				
Construction Testing Service	0.5%	0				
Owner's cost estimating / pr	LS	0				
Moving & equipment installa	LS	0				
Legal & Bridge Financing	5.0%	0				
Public Art @ 1%	0.0%	0				
					#VALUE!	#VALUE!
<b>7. Subtotal Project Costs</b>		\$0				
<b>8. Escalation Reserve @ 3%/yr</b>	mo.		To bid date			
				Totals	#VALUE!	#VALUE!
<b>Say</b>			<b>Say</b>		#VALUE!	#VALUE!

Updated revision 04

## PO Balance Summary

**Project Binder :** Ranger Reno-Durkee Brown      Harrington School of Communication  
**OCP Number:** KC.G.RANG.2007.001      [Agreement](#)  
**Excel Name:** Ranger Reno - Durkee Brown  
**Project Manager:** KB  
**Vendor:** Durkee Brown - V: #37247      **BID #:** 7037 URI Bid  
**PO Number:** 32732  
**PO Orgl Date:** 11/04/11      **EXP DATE:** 12/31/16  
**ACCOUNT #:** Multi      \$582,020.50      \$527,165.25 \$      54,855.25

DESCRIPTION & DATE	Date Rec'd in OCP	Date Paid	C.R. #	S.R. # & Date	PO AMOUNT	AMOUNT PAID	ACCOUNT BALANCE
Beginning Balance 10/19/11			15641		\$ 419,460.00		419,460.00
Inv. #1 11/01/11	11/16/11	12/30/11				\$19,602.06	399,857.94
Inv. #2 12/01/11 \$20,831.26	12/12/11						399,857.94
Inv. #2 01/01/12 \$19,526.07	01/17/12						399,857.94
Inv. #2 02/01/12	02/13/12	04/13/12				19,526.07	380,331.87
Inv. #3 (1129-3) 02/01/12	02/13/12	04/13/12				13,658.08	366,673.79
Inv. #4 (1129-4) 02/13/12	02/13/12	04/13/12				354.83	366,318.96
AOC 03/14/12 Fund Transfer			23350		-		366,318.96
Expense Transer 03/XX/12							366,318.96
Inv. #5 (1129-5) 03/01/12	03/26/12	04/27/12				17,375.50	348,943.46
Inv. #6 (1129-6) 04/01/12	05/16/12	06/15/12				18,912.29	330,031.17
Inv. #7 (1129-7) 05/01/12	05/16/12	06/29/12				12,047.49	317,983.68
Inv. #8 (1129-8) 06/11/12	06/19/12	07/06/12				16,889.56	301,094.12
Inv. #9 (1129-9) 07/31/12	08/16/12	10/05/12				9,663.23	291,430.89
Inv. #10 (1129-10) 10/01/12	10/08/12	11/23/12				1,653.00	289,777.89
AOC 11/07/12 Add'l Services	03/06/13		36429		111,361.00		401,138.89
Inv. #11 (1129-11) 12/01/12	12/19/12	01/11/13				5,486.25	395,652.64
Inv. #12 (1129-12) 03/01/13	03/01/13	04/19/13				12,982.70	382,669.94
Inv. #13 (1129-13) 04/01/13	04/08/13	05/17/13				9,541.90	373,128.04
Inv. #14 (1129-14) 05/01/13	05/24/13	06/25/13				9,813.81	363,314.23
Inv. #15 (1129-14) 06/01/13	06/11/13	07/12/13				49,001.83	314,312.40
Inv. #16 (1129-15) 06/30/13	06/12/13	07/19/13				23,936.41	290,375.99
Inv. #17 (1129-16) 09/01/13	11/11/13	12/16/13				122,878.09	167,497.90
Inv. #18 (1129-17) 11/30/13	12/30/13	01/27/14				29,431.00	138,066.90
AOC 01/08/14 - Addl Srvcs-Phase 1	02/20/14		58130		42,980.00		181,046.90
Inv. #19 (1129-19) 02/01/14	02/24/14	03/24/14				1,121.19	179,925.71
Inv. #20 (1129-20RT) 04/16/14	04/22/14	06/16/14				20,362.24	159,563.47
Inv. #21 (1129-21) 05/01/14	05/22/14	07/21/14				3,864.28	155,699.19
Inv. #22 (1129-22) 06/01/14	06/11/14	06/23/14				5,270.20	150,428.99
Inv. #23 (1129-23) 06/11/14	06/11/14	07/21/14				14,839.00	135,589.99
Inv. #24 (1129-24) 08/01/14	08/18/14	08/18/14				1,663.60	133,926.39
Inv. #25 (1129-25) 09/01/14	09/11/14	09/29/14				3,366.02	130,560.37
Inv. #26 (1129-26) 11/01/14	11/18/14	12/08/14				1,635.36	128,925.01
Inv. #27 (1129-27) 12/01/14	12/08/14	12/29/14				504.59	128,420.42
Inv. #28 (1129-28) 2/28/15	03/09/15	06/08/15				3,378.81	125,041.61
Inv. #29 (1129-30) 03/31/15	04/09/15	06/08/15				1,343.47	123,698.14
Inv. #30 (1129-31) 06/24/15	06/25/15	07/20/15				4,751.20	118,946.94
Inv. #31 (1129-32) 07/31/15	08/06/15	09/14/15				1,935.55	117,011.39
Inv. #32 (1129-33) 09/30/15	10/14/15	10/26/15				4,853.59	112,157.80
Inv. #33 (1129-34) 11/30/15	12/17/15	02/29/16				17,427.18	94,730.62
AOC Social Media Lab 106 & Screening/Lecture Room 103 rev			97553		8,219.50		102,950.12
Inv. #34 (1129-35) 12/31/15	03/16/16	04/18/16				13,866.05	89,084.07
Inv. #35 (1129-36) 02/29/16	03/16/16	04/18/16				7,449.62	81,634.45
Inv. #36 (1129-37) 04/30/16	05/17/16	06/27/16				20,958.10	60,676.35
Inv. #37 (1129-38) 06/30/16	06/20/16	07/25/16				5,821.10	54,855.25
							54,855.25
							54,855.25
<b>TOTALS</b>					<b>\$582,020.50</b>	<b>\$527,165.25</b>	<b>\$54,855.25</b>
						90.58%	

**Durkee Brown - V: #37247**  
**32732**  
**Account Breakdown**

Adam Roth - Com. Studies - Davis Hall

Vern  
 \$0.00                      \$0.00 \$                      -  
 Foundation-The Harrington School

874-9526  
 \$582,020.50                      \$527,165.25 \$                      54,855.25  
 Foundation-Harrington School Bldg

DESCRIPTION & DATE	9656-401-2135-G606			9656-401-2135-G510		
	FUNDING INCREASE	AMOUNT PAID	ACCOUNT BALANCE	FUNDING INCREASE	AMOUNT PAID	ACCOUNT BALANCE
Beg. Bal 10/19/11	\$ 419,460.00		\$ 419,460.00			\$0.00
Inv.#1 11/01/11		\$19,602.06	399,857.94			0.00
Inv.#2 12/01/11			399,857.94			0.00
Inv.#2 01/01/12			399,857.94			0.00
Inv.#2 02/01/12			399,857.94		19,526.07	-19,526.07
Inv.#3 02/01/12			399,857.94		13,658.08	-33,184.15
Inv.#4 02/13/12			399,857.94		354.83	-33,538.98
AOC 03/14/12	-399,857.94		0.00	399,857.94		366,318.96
Exp transfer 03/12/1	-19,602.06	-19,602.06	0.00	19,602.06	19,602.06	366,318.96
Inv. #5 03/01/12			0.00		17,375.50	348,943.46
Inv. #6 04/01/12			0.00		18,912.29	330,031.17
Inv.#7 05/01/12			0.00		12,047.49	317,983.68
Inv.#8 06/11/12			0.00		16,889.56	301,094.12
Inv.#9 07/31/12			0.00		9,663.23	291,430.89
Inv.#10 (1129-10) 10/01/12			0.00		1,653.00	289,777.89
AOC 11/30/12			0.00	111,361.00		401,138.89
Inv.#11 12/01/12			0.00		5,486.25	395,652.64
Inv.#12 03/01/13			0.00		12,982.70	382,669.94
Inv.#13 04/01/13			0.00		9,541.90	373,128.04
Inv.#14 05/24/13			0.00		9,813.81	363,314.23
Inv.#15 06/01/13			0.00		49,001.83	314,312.40
Inv. #16 06/30/13			0.00		23,936.41	290,375.99
Inv. #17 09/01/13			0.00		122,878.09	167,497.90
Inv. #18 11/30/13			0.00		29,431.00	138,066.90
AOC 11/20/13			0.00	42,980.00		181,046.90
Inv. #19 02/01/14			0.00		1,121.19	179,925.71
Inv. #20 04/16/14			0.00		20,362.24	159,563.47
Inv.#21 05/01/14			0.00		3,864.28	155,699.19
Inv.#22 06/01/14			0.00		5,270.20	150,428.99
Inv.#23 06/11/14			0.00		14,839.00	135,589.99
Inv.#24 08/01/14			0.00		1,663.60	133,926.39
Inv.#25 09/01/14			0.00		3,366.02	130,560.37
Inv.#26 11/01/14			0.00		1,635.36	128,925.01
Inv.#27 12/08/14			0.00		504.59	128,420.42
Inv.#28 2/28/15			0.00		3,378.81	125,041.61
Inv.#29 03/31/15			0.00		1,343.47	123,698.14
Inv.#30 06/24/15			0.00		4,751.20	118,946.94
Inv.#31 08/06/15			0.00		1,935.55	117,011.39
Inv.#32 09/30/15			0.00		4,853.59	112,157.80
Inv.#33 11/30/15			0.00		17,427.18	94,730.62
AOC			0.00	8,219.50		102,950.12
Inv.#34 12/31/15			0.00		13,866.05	89,084.07
Inv.#35 02/29/16			0.00		7,449.62	81,634.45
Inv.#36 04/30/16			0.00		20,958.10	60,676.35
Inv.#37 06/30/16			0.00		5,821.10	54,855.25
			0.00			54,855.25
			0.00			54,855.25
<b>TOTALS</b>			0.00			54,855.25
	\$0.00	\$0.00	\$ -	\$582,020.50	\$527,165.25	\$54,855.25

0

Trans Type	(All)
Budget Period	(All)

60,676.35	Total PS
-----------	----------

Line	Dist	Fund	Dept	Program	Monetary Amount
1					60,676.35
<b>Grand Total</b>					<b>60,676.35</b>



CO#	Proposed Amount	Description
12	\$ 8,186.00	Miscellaneous MEP Items
13	\$ 62,693.00	Revised Structural LVL's
14	\$ 7,600.00	Teaching Lecterns
15	\$ 30,000.00	Site Grading & Landscaping
16	\$ 1,000.00	Mullins & Crum Moving & Storage
17	\$ 3,084.00	Revised condensate pump feed
18	\$ 7,000.00	Roof ladder & Safety Post
19	\$ 5,000.00	Steam Trap Installation
20	\$ 15,000.00	Mechanical pad safety rail & screen
21	\$ 9,578.00	Elevate Electrical Pad
22	\$ 598,228.00	New Sprinkler System
23	\$ 44,240.00	Cleaning out casework & materials



0

**\*\* Double click on the line number to view distribution and chartfiled info for that line. Double click again to hide detail.  
\*\* Double click on a line amount to drill down to all items proce**

Trans Type	(All)
Budget Period	(All)

**(823,564.21) Total PS**

Line	Dist	Fund	Dept	Program	Monetary Amount
<b>1</b>					<b>2,022,975.00</b>
<b>Grand Total</b>					<b>2,022,975.00</b>

University of Rhode Island  
Sample Project

Start Date 1/1/2016  
Finish Date 30 6/22/2018

**Project Budget**

March 11, 2014  
August 15, 2016

**Program SF**

12,414 GSF  
8,690 NASF  
0 GSF  
GSF  
Total Program  
Shelled  
Renovated  
70% Efficiency  
Demolished

1. General Construction Costs

Estimate

New Construction	\$300 /SF	3,724,286	New Construction
Renovation	\$150 /SF	0	Renovated space
Credit for shelled space	-\$100 /SF	0	Shelled space
Design Contingency	5.0%	186,214	
Estimating Contingency	10.0%	391,050	
Construction Contingency	6.0%	258,093	
<b>Building Construction Cost</b>		<b>\$4,559,643</b>	<b>= \$367.29 /SF</b>

2. Site Preparation - Demolition and Landscaping

Building Demolition	LS	20,000	
Temporary Construction	LS	25,000	
On-site utilities	1.00%	45,596	% of Building Construction Cost
New Parking	1 space /350SF	N/A	@ \$2,200/space N/A Spaces
Replacement Parking	20	44,000	@ \$2,200/space
Hardscape	2.0%	91,193	% of Building Construction Cost
Landscaping	1.0%	45,596	% of Building Construction Cost
Construction Contingency	6.0%	16,283	
<b>Site Development</b>		<b>\$287,669</b>	

3. Escalation Reserve

Escalation @ 4.5%/yr for 2014	12 mo.	\$222,685	
Escalation @ 5%/yr for 2015 on	30 mo.	\$673,570	
<b>Total Escalation</b>	<b>42 mo.</b>	<b>\$896,255</b>	<b>Sum construction = \$5,743,567</b>
			<b>Total without construction contingency \$5,469,191</b>

4. Building Design Fees and Testing Services

Programming		In Basic Fee	
Geotechnical Drilling & Report		In additional Services	
Basic Fee	LS	301,500	
Additional Consultants	LS	203,810	
Additional Services	LS	90,000	
Reimbursables & Expenses	LS	15,000	
Fees & Services Contingency	5.0%	30,516	
<b>Total Building Design Fees &amp; Testing Services</b>		<b>\$640,826</b>	<b>Percent of Construction = 11.16%</b>

5. Site Development Contribution - Non Site Specific

Utilities ( water, gas, storm, steam)	LS	0	
Electrical Substation contribution	LS	0	
Utilities Engineering	LS	0	
Campus Master Planning contribution	0.00%	0	% x Construction
<b>Total Site Development</b>		<b>\$0</b>	<b>Sum Site Development = \$0</b>

6. Equipment & Furnishings

Telephone/Data equipment	LS	50,000	Cabling in building cost
Security systems	LS	15,000	Cabling in building cost
Furniture & Fixtures	\$12 SF	148,971	Loose furniture & equipment
Laboratory Equipment	LS	0	NIC
Other Equipment (N.I.C.)	LS	400,000	A/V Technology
<b>Total Equipment</b>		<b>\$613,971</b>	

7. Legal/Administrative Costs

Building Commissioning	0.6%	34,461	Est. URI contract
Building Permit	0.3%	17,231	Est. Building only
Fire Marshall review	fee	24,007	Building only
Liability Insurance OCIP Contribution	0.0%	0	Included in GC budget above
Builder's Risk insurance	0.1%	5,744	
Project Management (Design)	LS	99,812	CP&D contract staff & operations
Project Management (Construction)	5.0%	287,178	OCP contract staff & operations
Construction Testing Services	0.3%	17,231	URI contract
Owner's cost estimating / preconstruction	LS	25,000	URI consultant
Moving & equipment installation	LS	25,000	
Legal & Bond fees	0.0%	0	% x Construction
Public Art @ 1%	0.0%	0	1% Building construction
<b>Legal/Administrative costs</b>		<b>\$535,664</b>	<b>Funding Fund Balance</b>

8. Subtotal Project Costs

<b>Project Estimate w/ Escalation</b>	<b>\$7,534,028</b>	<b>Contingency in above = \$882,156</b>
<b>Say</b>	<b>\$7,600,000</b>	

## Copyright

© 2016 The Santa Fe Group, Shared Assessments Program. All rights reserved.

Documents created under the Shared Assessments Program may be downloaded from the official Shared Assessments Program website at [www.sharedassessments.org](http://www.sharedassessments.org).

While retaining copyrights, the Shared Assessments Program makes specific documents available to members and purchasers for the purpose of conducting self-assessments and third party security assessments. Licenses for other uses are available from Shared Assessments. Individuals and organizations should review the terms of use prior to downloading, copying, using or modifying Shared Assessment Program documents.

This notice must be included on any copy of the Shared Assessments Program documents, excluding assessors or consultants' reports.

The Shared Assessments Program is administered by The Santa Fe Group ([www.santa-fe-group.com](http://www.santa-fe-group.com)). Questions about this document and the program should be directed to [info@sharedassessments.org](mailto:info@sharedassessments.org).

## Terms of Use

### 2017 SHARED ASSESSMENTS STANDARDIZED INFORMATION GATHERING (SIG) QUESTIONNAIRE (2017 SIG)


The Shared Assessments Program ("Program") maintains, promotes and facilitates the use of the Standardized Information Gathering ("SIG") questionnaire 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](mailto: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 AUP 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.

THE SHARED ASSESSMENTS PROGRAM DOCUMENTS ARE PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED. IN NO EVENT SHALL THE SANTA FE GROUP, OR THE SHARED ASSESSMENTS PROGRAM, ITS SPONSORS OR PROGRAM MEMBERS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THE SHARED ASSESSMENTS PROGRAM DOCUMENTS, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.



**SHARED ASSESSMENTS**

**2017 SHARED ASSESSMENTS STANDARDIZED INFORMATION GATHERING (SIG) QUESTIONNAIRE (2017 SIG) Lite**  
**Version 2017**  
**Released: November 2016**

<http://www.sharedassessments.org>  
[sharedassessments@santa-fe-group.com](mailto:sharedassessments@santa-fe-group.com)

Initiator Information

**Assessee Instructions**

Review the request provided by your client/customer which should provide you with instructions on how to answer the SIG and detail the sections of the SIG you are required to complete. In addition, your client/customer should provide you with the scope of services for which to provide responses. If you did not receive instructions or scope from your client we recommend you contact them and seek guidance on how they need the SIG answered and the sections they require you to complete.

Primary or parent questions are followed by numbered sub or child questions. The SIG has built-in automation. Based on your responses, cells will change color or if Excel macros are enabled child questions may not be displayed. This will reduce the number of questions you are required to complete. When you answer No or N/A to a question in a cell, all of its related sub-questions will either be hidden and/or the response field will change color identifying that question has been answered. The issuer will see only the No or N/A response for the parent and all of its child questions. If your client/customer requests a maturity response, for all Yes responses you must provide a Maturity value for that question in the Maturity column. The Maturity levels are provided when the cell is selected.

There are two parts to this questionnaire:  
 - SIG Lite  
 - Detail tabs (A through U)

The instructions below will help you in the completion of the SIG Lite or full SIG.

**SIG Lite**

- 1) Complete the "Business Information" tab.
- 2) Compile the documentation requested on the "Documentation" tab.
- 3) Answer all of the questions on the "SIG Lite" tab by selecting Yes, No or N/A from the drop-down menu.
- 4) Use the "Additional Information" field to provide any pertinent information. (An explanation is required for N/A responses.)
- 5) Answer questions on the "Additional Questions" tab (tab Z) only if additional questions have been inserted.

**Note:** Answers provided in the Lite tab are automatically transferred to the corresponding tab in the full SIG avoiding the need to answer those questions again.

**Issuer/Outsourcer Instructions**

We recommend that prior to issuing the SIG you review which sections of the SIG your vendor should answer based on the type of service(s) they provide. We recommend that along with the SIG, you notify them of the sections they are required to complete and any other information required to accurately complete the SIG (additional questions, documents, etc.).

Detailed instructions on how to use the SIG are contained in the How To Guide which you may want to provide along with the SIG.

**SIG Management Tool (SMT)**

A macros-enabled spreadsheet is provided to Issuers of the SIG to help with processing service provider responses and managing the transfer of responses from previous versions of the SIG. If a master SIG is created, the SMT allows for comparisons of all responses in the master SIG to the SIG offered by a service provider. The SMT will also transfer responses and the "Additional Information" field from previous versions of the SIG. For a full list of functions, please refer to the SMT Functionality tab.

**Note:** Detailed instructions for the use of the SMT are included in the How To Guide.

## Dashboard

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

Tabs	% Comp	Response Cell Background Color Coding (All tabs)	Resp
<a href="#">Copyright</a>	N/A	Response Required (all cells with a blue background are editable)	
<a href="#">Terms of Use</a>	N/A	Yes Response	<b>Yes</b>
<a href="#">Instructions</a>	N/A	No Response	<b>No</b>
<a href="#">Business Information</a>	0%	N/A Response	<b>N/A</b>
<a href="#">Documentation</a>	N/A	Top of table (no response required)	
<a href="#">SIG Lite</a>	0%		
<a href="#">Z. Additional Questions</a>	N/A		
<a href="#">Glossary</a>	N/A		
<a href="#">Formula Notes</a>	N/A		
<a href="#">Full</a>	N/A		
<a href="#">Full Lite</a>	N/A		
<b>SIG Total</b>	0%		

<b>Business Information</b>	
<b>0% Percent Complete</b>	
<b>Question/Request</b>	<b>Response</b>
Assessee Name	
Assessee Job Title	
Assessee Contact Information	
Names and titles/functions of individuals who contributed to this questionnaire	
Date of Response	
<b>Company Profile</b>	
Name of the holding or parent company	
Company/business name	
Publicly or privately held company	
If public, what is the name of the Exchange	
If public, what is the trading symbol	
Type of legal entity and state of incorporation	
How long has the company been in business	
Are there any material claims or judgments against the company	
If yes, describe the impact it may have on the services in scope of this document	
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.	
<i>Scope</i>	
<i>Please provide the below responses to establish the scope of the SIG</i>	
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.	
Are software applications provided?	
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?	
Commercial Off-The-Shelf (COTS)	
Custom Developed	
Cloud	
Mobile	
Open Source Software	
Other	



## Documentation\*

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

Document Request	Question Reference	Name and/or type of information provided (e.g., document, summary, table of contents)
* Information Security policies and procedures. This should include the following (if not, provide the individual documents as necessary): a) Hiring policies and practices and employment application b) User Account administration policy and procedures for all supported platforms where Scoped Systems and Data are processed and network/LAN access c) Supporting documentation to indicate completion of User Entitlement reviews d) Employee Non-disclosure agreement document e) Information Security Incident Report policy and procedures, including all contract information f) Copy of Visitor policy and procedures g) Security Log Review policies and procedures h) Copy of third party risk management policies and procedures		
* Copy of internal or external information security audit report		
Information technology and security organization charts (including where Respondent information security resides and the composition of any information security steering committees). Note: Actual names of employees are not required		
* 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 of systems, applications, and networks		
* Software development and lifecycle (SDLC) process document		
* Business Resiliency (continuity plan) (BCP) and/or Disaster Recovery Plan		
* Most recent BCP/DR test dates and results		
* Most recent AUP/SSAE16/SOC2 audit report(s)		
* Privacy Policies (internal, external, web)		
* Executive Summary of certificates held. (e.g. PCI, HIPAA, ISO)		
* Performance Reports against contracted SLAs		

\*If the Respondent 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.

**SIG Lite** 0% Percent Complete 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 and disable the transfer of responses from the Lite 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.

Ques Num	Question/Request	Response	Maturity	Additional Information	AUP Reference	ISO 27002:2013 Relevance
<b>A. Risk Assessment and Treatment</b>						
SL.1	Is there a risk assessment program that has been approved by management, communicated to constituents and an owner to maintain and review the program? if yes, does it include:				A.1 IT & Infrastructure Risk Governance and Context	5.1 6.1.2 Leadership & Commitment, Information Security Risk Assessment
SL.8	Do Subcontractors have access to Scoped Systems and Data? (backup vendors, service providers, equipment support maintenance, software maintenance vendors, data recovery vendors, etc.)? If yes, is there:					15 Supplier relationships
SL.9	A documented vendor management process in place for the selection, oversight and risk assessment of third party vendors? If yes, does it include:				A.7 Subcontractor Selection and Management Process	15.1.1 Information security policy for supplier relationships
SL.15	Is there a vendor management program?				A.5 Vendor Risk Management Program	
SL.16	Do external parties have access to Scoped Systems and Data or processing facilities?					15 Supplier relationships
SL.17	Is the maturity of IT management processes formally evaluated at least annually using an established benchmark (e.g., COBIT maturity models)?					17.1.3 Verify, review and evaluate information security continuity
SL.18	Are there regular privacy risk assessments conducted? If yes, provide frequency and scope. If no, explain reason.				P.3 Privacy Organization and Program Maintenance	15.1.3.i Information and communication technology supply chain
SL.19	Are identified privacy risks and associated mitigation plans formally documented and reviewed by management?				P.3 Privacy Organization and Program Maintenance	15.1.1.i Information security policy for supplier relationships
SL.20	Are reasonable resources (in time and money) allocated to mitigating identified privacy risks?				P.3 Privacy Organization and Program Maintenance	
SL.21	Is there a compliance risk management system that addresses the quality and accuracy of reported consumer data?				P.3 Privacy Organization and Program Maintenance	
SL.22	Is there a compliance risk management system that addresses the quality of assembling and maintaining the data?				P.3 Privacy Organization and Program Maintenance	
<b>B. Security Policy</b>						
SL.23	Is there an information security policy that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?				B.1 Information Security Policy Maintenance	5.1.1 Policies for information security
SL.24	Have the policies been reviewed in the last 12 months?				B.1 Information Security Policy Maintenance	5.1.2 Review of the policies for information security
<b>C. Organizational Security</b>						
SL.25	Is there a respondent information security function responsible for security initiatives?				C.1 Security Organization Roles / Responsibilities	6.1.1 Information Security Roles and Responsibilities
<b>D. Asset and Information Management</b>						
SL.26	Is there an asset management policy approved by management, communicated to constituents and an owner to maintain and review?				D. Asset and Information Management	8.1 Responsibility for Assets
SL.27	Is information classified?				D.1 Asset Accounting and Inventory	8.2.1 Classification of Information
SL.28	Is there a removable media policy or program (CDs, DVDs, tapes, disk drives) that has been approved by management, communicated to appropriate constituents, and an owner to maintain and review the policy?				D.4 Removable Device Security	8.3.1 Management of Removable Media

Ques Num	Question/Request	Response	Maturity	Additional Information	AUP Reference	ISO 27002:2013 Relevance
SL.29	Is Scoped Data sent or received via physical media?				D.2 Physical Media Tracking	8.3.3 Physical Media in Transit
SL.30	Are encryption tools managed and maintained for Scoped Data? If yes:				D.5 Data Security Policy - Encryption	10.1 Cryptographic controls
SL.31	Are clients provided with the ability to generate a unique encryption key?				D.5 Data Security Policy - Encryption	10.1.2 Key Management
SL.32	Are clients provided with the ability to rotate their encryption key on a scheduled basis?				D.5 Data Security Policy - Encryption	10.1.2 Key Management
SL.33	Are staff able to access client Scoped Data in an unencrypted state?				H.3 Logical Access Authorization	9.2.3 Management of privileged access rights 9.4.6 Information access restriction
SL.34	Are staff able to access client's encryption keys?				H.3 Logical Access Authorization	9.2.3 Management of privileged access rights 9.4.7 Information access restriction
SL.35	Is data segmentation and separation capability between clients provided?				V.1 Service and Deployment Models	9.4.1 Information access restriction
SL.36	Does the ability exist to legally demonstrate sufficient data segmentation, in the event of a client subpoena or a forensics incident, so as not to impact other clients data if using resource pooling?				V.1 Service and Deployment Models	16.1.1 Responsibilities and Procedures, 16.1.7 Collection of Evidence.
SL.37	Is there a data classification retention program that identifies the data types that require additional management and governance?				P.1 Scoped Privacy Data Inventory and Flows	8.2 Information Classification
SL.38	Is there a self-service portal or API call available to clients which provides the ability to place a "Legal hold" on client data which may be subject to a legal action, without impacting other clients data retention or destruction schedules?				P.6 Management of Client Scoped Privacy Data	16.1.1 Responsibilities and Procedures, 16.1.7 Collection of Evidence, 18.1.2 Intellectual Property Rights, 18.1.3 Protection of records
<b>E. Human Resource Security</b>						
SL.39	Is there a Human Resource policy approved by management, communicated to constituents and an owner to maintain and review? If yes, does it include:					
SL.46	Are background checks performed for Service Provider Contractors and Subcontractors?				E.2 Background Investigation Policy Content	7.1.1 7.2.1 Screening Management responsibilities
SL.47	Do information security personnel have professional security certifications?					6.1.4 Contact with special interest groups
<b>F. Physical and Environmental Security</b>						
SL.48	Is there a physical security program?				F.2 Physical Security Controls - Scoped Data	5.1.1 Policies for information security
SL.49	Are physical security and environmental controls in the data center and office buildings?				F. Physical and Environmental Security	11.1 Secure areas
SL.50	Are visitors permitted in the facility?				F.7 Visitor Management	11.1.2 Physical entry controls
<b>G. Operations Management</b>						
SL.51	Are management approved operating procedures utilized?				G. Operations Management	12.1.1 Documented Operating Procedure
SL.52	Is there an operational change management/change control policy or program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?				G.1 Change Control	12.1.2 Change Management
SL.53	Are backups of Scoped Systems and Data performed?				K.5 Backup Media Restoration	12.3.1 Information Back-Up
SL.54	Are Cloud Services provided? If yes, what service model is provided (select all that apply):				V.1 Service and Deployment Models	4.3 Determining the scope of the information management system

Ques Num	Question/Request	Response	Maturity	Additional Information	AUP Reference	ISO 27002:2013 Relevance
SL.61	Is there a client management portal which allows distributed business accounts (business units/departments) to be managed under a single central corporate account?					15.2.1 Monitoring and review of supplier services
SL.62	Are application self service features or an Internet accessible self-service portal available to clients?					9.4.1 Information access restriction
SL.63	Can clients run their own security services within their own cloud environment?				V.3 Cloud Audit Program	12.4.1 Event logging, Administrator and operator logs, Control of operational software, 12.5 Management of technical vulnerabilities, 12.6.1
SL.64	Is there a management approved process to ensure that image snapshots containing Scoped Data are authorized prior to being snapped?					9.2.3 Management of privileged access rights
SL.65	Is there a formal process to ensure clients are notified prior to changes being made which may impact their service? If yes, what is the communication method:				G.1 Change Control	12.1.2 Change management
SL.66	Is there a scheduled maintenance window? If yes, what is the frequency:				V.4 Security Review of Hypervisor Configuration	12.6.1 Management of technical vulnerabilities
SL.67	Is there a scheduled maintenance window which results in client downtime? If yes, what is the downtime:				V.4 Security Review of Hypervisor Configuration	14.2.2.1 System change control procedures
SL.68	Is there an online incident response status portal, which outlines planned and unplanned outages? If yes, how long after an unplanned outage is this updated:				J. Incident Event and Communications Management P.8 Privacy Incident Notification and Response Management	14.2.2 System change control procedures
<b>H. Access Control</b>						
SL.69	Are electronic systems used to transmit, process or store Scoped Systems and Data?					
SL.70	Are individual IDs required for user authentication to applications, operating systems, databases and network devices?				H.1 Password Controls	9.2.1.a User registration and de-registration
SL.71	Are passwords used?				H. Access Control	
SL.72	Is there a password policy for systems that transmit, process or store Scoped Systems and Data that has been approved by management, communicated to constituents, and enforced on all platforms?				H. Access Control	9.4.3 Password Management System
SL.73	Is remote access permitted?				H.8 Restrictions and Multifactor Authentication	6.2 Mobile devices and teleworking
SL.74	Is standards based federated ID capability available to clients (e.g., SAML, OpenID)?					9.2.1 User registration and de-registration
SL.75	Is two factor authentication required to access the production environment containing Scoped Data?					9.3.1 Use of secret authentication information
SL.76	Are staff able to access client Scoped Data? If not, please identify the controls used to prevent this.				H.3 Logical Access Authorization	9.2.3 Management of privileged access rights 9.4.1 Information access restriction
SL.77	Is there a process which allows the client to specifically list who from the provider will have access to their Scoped Systems and Data?				H.3 Logical Access Authorization	9.1.1 9.2.3 Access Control Policy Management of privileged access rights
<b>I. Application Security</b>						
SL.78	Are applications used to transmit, process or store Scoped Data?				I.1 Application Security Program Governance	
SL.79	Is a web site supported, hosted or maintained that has access to Scoped Systems and Data?					
SL.86	Is application development performed?				I. Application Security	

Ques Num	Question/Request	Response	Maturity	Additional Information	AUP Reference	ISO 27002:2013 Relevance
SL.96	Are applications analyzed on a regular basis to determine their vulnerability against recent attacks?				I.10 QA_UAT Process	12.2.1 Controls against malware
SL.97	Is there a formal development methodology in operation? If yes, which groups does it include?:				I.16 Secure Systems Development Lifecycle (SDLC) Reviews	12.5.1 Control of Operational Software
SL.98	Are mobile applications that access Scoped Systems and Data developed?					
<b>J. Incident Event and Communications Management</b>						
SL.99	Is there an Incident Management Program that has been approved by management, communicated to constituents and an owner to maintain and review the program? If yes, does the program include:				J.1 Information Security / Information Technology Incident Management - Policy and Procedures Content	16 Information security incident management
SL.101	Is there a formal Incident Response Plan?				J. Incident Event and Communications Management	16.1.1.a.1 Responsibilities and procedures
SL.102	Is there a 24x7x365 staffed phone number available to clients to report security incidents?				J. Information Security Incident Management P.8 Privacy Incident Notification and Response Management	15.1.1.h Information security policy for supplier relationships
<b>K. Business Resiliency</b>						
SL.103	Is there an established Business Resiliency program that has been approved by management and communicated to appropriate constituents?				K.1 Business Resiliency Governance	5.2 Management Commitment
SL.104	Has a Business Impact Analysis been conducted?				K.2 Business Impact Analysis	8.2.2 Business impact analysis
SL.105	Is there a formal process focused on identifying and addressing risks of disruptive incidents to the organization?				K.3 Risk Assessment	8.2.3 Risk assessment
SL.106	Are specific response and recovery strategies defined for the prioritized activities?				K.4 Business Activity level Recovery Planning	8.3.1 Determination and selection
SL.107	Are formal business continuity procedures developed and documented?				K.4 Business Activity level Recovery Planning	8.4 Establish and implement business continuity procedures
SL.108	Has senior management assigned the responsibility for the overall management of the response and recovery efforts?				K.1 Business Resiliency Governance	
SL.109	Is there a periodic (at least annual) review of your Business Resiliency Program?				K.6 Exercising	8.4.1 Establish and implement business continuity procedures
SL.110	Are there any dependencies on critical third party service providers?				K.2 Business Impact Analysis	8.1 Operational Planning and Control 8.3 8.3.1 Business continuity strategy 8.44 Determination and selection Business continuity plans
SL.111	Is there a formal, documented exercise and testing program in place?				K.6 Exercising	8.5 Exercising and testing
SL.112	Is there an Influenza Pandemic / Infectious Disease Outbreak Plan?				K.7 Infectious Disease Planning	
SL.113	Is there a specific Recovery Time Objective (RTO)? If yes, what is it?					17.1.2 Implementing information security continuity

Ques Num	Question/Request	Response	Maturity	Additional Information	AUP Reference	ISO 27002:2013 Relevance
SL.114	Are all suppliers of critical hardware, network services and facility services involved in annual continuity and recovery tests?					17.1.3 Verify, review and evaluate information security continuity
SL.115	Are site failover tests performed at least annually?					17.1.3 Verify, review and evaluate information security continuity
SL.116	Do contracts with Critical Service Providers include a penalty or remediation clause for breach of availability and continuity SLAs?					15.1.2 15.2.1 Addressing security within supplier agreements, Monitoring and review of supplier services
SL.117	Is there sufficient redundancy capacity to ensure services are not impacted in multi-tenancy environments during peak usage and above?					17.1.3 Verify, review and evaluate information security continuity
<b>L. Compliance</b>						
SL.118	Is there an internal audit, risk management, or compliance department, or similar management oversight unit with responsibility for assessing, identifying and tracking resolution of outstanding regulatory issues?				L.3 Monitoring and Reporting - Compliance Requirement Identification	18.1.1 Identification of applicable legislation and contractual requirements
SL.119	Are there policies and procedures to ensure compliance with applicable legislative, regulatory and contractual requirements including intellectual property rights on business processes or information technology software products?				L.2 Monitoring and Reporting - Compliance	
SL.120	Is there a records retention policy covering paper and electronic records, including email in support of applicable regulations, standards and contractual requirements?					18.1.3 Protection of records
SL.121	Is licensing maintained in all jurisdictions where required?					
SL.122	Is there an documented internal compliance and ethics program to ensure professional ethics and business practices are implemented and maintained?				L.4 Professional Ethics and Business Practices	
SL.123	Are marketing or selling activities conducted directly to Client's customers?					
SL.124	Are there direct interactions with your client's customers?					
SL.125	Are documented policies and procedures maintained for enabling compliance with applicable legal, regulatory, or contractual obligations related to information security requirements?					
SL.126	Is there a documented governance process to identify and assess changes that could significantly affect the system of internal controls for security, confidentiality and availability?				L.3 Monitoring and Reporting - Compliance Requirement Identification	
SL.127	Are accounts opened, transactions initiated or other account initiation activity applying payments, taking payments, transferring funds, etc. through either electronic, telephonic, written or in-person requests made on behalf of your client's?					
SL.128	Are these sites, applications and systems used to also transmit, process or store non-scoped data?					
SL.129	Are all transaction details (such as payment card info and information about the parties conducting transactions) prohibited from being stored in the DMZ?					14.1.3.e Protecting Application Services Transactions
SL.130	Does the service provider permit client audits and assessments?				V.3 Cloud Audit Program	15.1.2 15.2.1 Addressing security within supplier agreements, Monitoring and review of supplier services
<b>M. End User Device Security</b>						

Ques Num	Question/Request	Response	Maturity	Additional Information	AUP Reference	ISO 27002:2013 Relevance
SL.131	Are End User Devices (Desktops, Laptops, Tablets, Smartphones) used for transmitting, processing or storing Scoped Data? If yes, for all platforms, are:					
SL.136	Are constituents allowed to utilize mobile devices within your environment? If yes, which of the following functions are allowed:					
SL.141	Is there a mobile device management program in place that has been approved by management and communicated to appropriate constituents?					
SL.144	Are staff technically prevented from accessing the administrative environment via non-managed private devices? If yes, is it from:				H.3 Logical Access Authorization	9.1.1 9.1.2 9.2.1 9.2.3 Access control policy, Access to networks and network services, User registration and de-registration, Management of privileged access rights
<b>N. Network Security</b>						
SL.145	Are there external network connections (Internet, extranet, etc.)?				B.2 Information Security Standards N.Network Security	13.1.1 Network Controls
SL.146	Security and hardening standards for network devices, including Firewalls, Switches, Routers and Wireless Access Points (baseline configuration, patching, passwords, access control)?				N. Network Security	13.1.1.c Network Controls
SL.147	Are firewalls used to isolate critical and sensitive systems into network segments separate from network segments with less sensitive systems?				N.2 Network Security - Firewall(s) and/or Other Devices Providing the Same Functionality	13.1.3 Segregation In Networks
SL.148	Is there a process that requires security approval to allow external networks to connect to the company network, and enforces the least privilege necessary?					9.1.2.b Access to networks and network services
SL.149	Are all available high-risk security patches applied and verified at least monthly?					12.6.1.g Management of technical vulnerabilities
SL.150	Are Intrusion Detection/Prevention Systems employed in all sensitive network zones and wherever firewalls are enabled?				N.3 Network Security - IDS/IPS Attributes	13.1.2 Security of Network Services
SL.151	Are wireless networking devices connected to networks containing scoped systems and data?				N.7 Unauthorized Wireless Networks	13.1.1.c Network Controls
SL.152	Are there controls to prevent one client attempting to compromise another client in a resource pooled environment?				H.3 Logical Access Authorization	12.4.1 Event Logging, 15.2.1 Monitoring and review of supplier services
<b>P. Privacy</b>						
SL.153	Is Scoped Data transmitted, processed, or stored that can be classified as non-public information (NPI), personally identifiable information (PII), or sensitive customer financial information? If yes, describe and list types of data.					8.2.1 Classification of Information
SL.154	Do agreements with third parties who have access or potential access to Scoped Data, address confidentiality, audit, security, and privacy, including but not limited to incident response, ongoing monitoring, data sharing and secure disposal of Scoped Data?				P.4 Third Party Privacy Agreements	15.1.2 Addressing security within supplier agreements
SL.155	Is a business associate contract in place to address obligations for the privacy and security requirements for the services provided?				P.4 Third Party Privacy Agreements	15.1.2 Addressing security within supplier agreements
SL.156	For Scoped Data, is personal information about individuals transmitted to or received from countries outside the United States? If yes, list the countries.					
SL.157	Is personal information transmitted, processed, stored, or disclosed to or retained by third parties? If yes, describe.					15 Supplier Relationships



Ques Num	Question/Request	Response	Maturity	Additional Information	AUP Reference	ISO 27002:2013 Relevance
SL.161	Are transactions for covered accounts accessed, modified, or processed, including address changes and discrepancies? If yes, describe.					
<b>T. Threat Management</b>						
SL.162	Is there an anti-malware policy or program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?				T.1 Virus Protection (Servers) T.2 Virus Protection (Workstations)	12.2.1 Controls Against Malware
SL.164	Is there a vulnerability management policy or program that has been approved by management, communicated to appropriate constituents and an owner assigned to maintain and review the policy?				T.4 Technical Compliance Checking - Vulnerability Testing and Remediation	12.6.1 Control of technical vulnerabilities
SL.165	Are vulnerability scans performed on all internet-facing applications at least monthly and after significant changes?				T.3 Application Vulnerability Assessments/Ethical Hacking	12.6.1 Management of technical vulnerabilities
SL.166	Are vulnerability scans performed against internal networks and systems?					
SL.167	Are penetration tests performed?					
SL.168	Are there processes to manage threat and vulnerability assessment tools and the data they collect?				I.1 Application Security Program Governance	12.6.1 Management of technical vulnerabilities
<b>U. Server Security</b>						
SL.169	Are Servers used for transmitting, processing or storing Scoped Data?					
SL.170	Are systems and applications patched?				G.2 System Patching	12.6.1 Management of technical vulnerabilities
SL.171	Are default hardened base virtual images applied to virtualized operating systems?				U.2 System Hardening Standards	
SL.172	Are Hypervisors used to manage systems used to transmit, process or store Scoped Data?				V.4 Security Review of Hypervisor Configuration	14.1.2 Securing application services on public networks

## Z. Additional Questions

This tab is used to supply any additional questions not covered by this SIG. Questions on this tab will not be analyzed by the SIG Management Tool.

Ques Num	Question/Request	Response	Additional Information	AUP Reference	ISO Ref Num	ISO Ref Text
----------	------------------	----------	------------------------	---------------	-------------	--------------

<b>Glossary</b>		
<b>Term</b>	<b>Definition</b>	<b>Source</b>
<b>Acceptable Use Policy</b>	Part of the information security framework that defines what users are and are not allowed to do with the IT systems of the respondent. It should contain a subset of the information security policy and refer users to the full security policy when relevant. It should also clearly define the sanctions applied if a user violates the policy.	
<b>Access</b>	Obtaining, retrieving, altering, duplicating, copying, scanning, photographing, using, disclosing, examining, printing, reading, and/or viewing Scoped Data stored in any media including but not limited to paper, x-ray, film, a computer's memory, and electronic media such as an internal or external hard drive, a backup tape, or a USB stick. Viewing, photographing, altering, printing, using, and/or disclosing, Scoped Data displayed on a computer monitor, screen, or any other device such as a smartphone, tablet, and the like. (See also Potential Access)	
<b>Accountability</b>	The obligation of an individual or organization to account for its activities, accept responsibility for all success and failures associated with the activity and to disclose the results in a transparent and timely manner.	
<b>Acknowledgement of Acceptable Use</b>	A written attestation from a user of an information system indicating the user's acceptance and willingness to comply with the relevant information systems control policies.	
<b>ACL (Access Control List)</b>	A list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects.	Wikipedia
<b>Anti-Tailgating / Anti-Piggybacking Mechanism</b>	Two sets of doors whereby access to the second is not granted until the individual has passed through (and closed) the first, often referred to as a "man trap." A controlled turnstile is also considered an anti-tailgating/piggybacking mechanism.	
<b>API</b>	Application program interface (API) is a set of routines, protocols, and tools for building software applications. An API specifies how software components should interact and APIs are used when programming graphical user interface (GUI) components.	Webopedia
<b>Applicable Privacy Law</b>	Relevant laws, enactments, regulations, binding industry codes, regulatory permits and licenses that are in effect and address the protection, handling and privacy of scoped privacy data, selected as being in scope for the assessment.	
<b>Application Inventory System</b>	An asset-based approach that includes an itemized list of applications or application components, such that software versions, security testing results and additional attributes can be individually identified against such assets.	
<b>Application Segmentation</b>	In response to the advent of borderless applications, application segmentation has evolved and should be applied consistently on the application no matter where it goes, which borders it crosses, or which siloes are carrying its traffic. In enterprises where segmentation is oriented around applications instead of infrastructure, the security benefit is immediately apparent. If a hacker manages to compromise a user, then the hacker's access is contained and limited to only the applications that the compromised user is allowed to access. They cannot move laterally or hop from application to application, browsing through the IT infrastructure until they find the most sensitive or valuable applications and data. The data breach is, by default, contained and cannot spread.	<a href="http://www.cloudstrategymag.com/articles/85958-application-segmentation">http://www.cloudstrategymag.com/articles/85958-application-segmentation</a>
<b>Asset</b>	In computer security, a major application, general-support system, high-impact program, physical plant, mission-critical system, personnel, equipment, or a logically related group of systems.	NIST: CNSSI-4009
<b>Asset Classification</b>	The category or type assigned to an asset, which is derived from the asset classification policy. Asset classifications frequently vary from company to company.	
<b>Asset Control Tag</b>	A unique identification number assigned to all inventoried assets.	
<b>Asset Management Program</b>	A program for managing an organization's assets which includes formalized governance, policies, and procedures.	
<b>Asset Tracking</b>	Asset tracking refers to the method of tracking physical assets, either by scanning barcode labels attached to the assets or by using tags using GPS or RFID which broadcast their location.	Wikipedia
<b>Attack Vector</b>	Path or means by which an attacker can gain access to a system or network in order to deliver a payload or malicious outcome.	
<b>Attribute</b>	A property or field of a particular object.	

Term	Definition	Source
<b>Authentication</b>	The process of verifying the identity of an individual user, machine, software component, or any other entity	FFIEC Information Security Booklet
<b>Baseline</b>	A benchmark by which subsequent items are measured.	
<b>Battery</b>	An electrochemical cell (or enclosed and protected material) that can be charged electrically to provide a static potential for power or released electrical charge when needed.	
<b>Biometric Reader</b>	A device that uses measurable biological characteristics such as fingerprints or iris patterns to assist in authenticating a person to an electronic system.	
<b>Business Associate</b>	<p>A business associate is a person or organization, other than an employee of a covered entity, that performs certain functions on behalf of, or provides certain services to, a covered entity that involve access to PHI. A business associate can also be a subcontractor responsible for creating, receiving, maintaining, or transmitting PHI on behalf of another business associate. Business associates provide services to covered entities that include:</p> <ul style="list-style-type: none"> <li>Accreditation</li> <li>Billing</li> <li>Claims processing</li> <li>Consulting</li> <li>Data analysis</li> <li>Financial services</li> <li>Legal services</li> <li>Management administration</li> <li>Utilization review</li> </ul> <p>NOTE: A covered entity can be a business associate of another covered entity.</p>	<a href="https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/HI/PAAPrivacyandSecurity.pdf">https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/HI/PAAPrivacyandSecurity.pdf</a>
<b>Business Continuity</b>	A set of planning, preparatory and related activities which are intended to ensure an organization's critical business functions will either continue to operate despite serious incidents or disasters that might otherwise have interrupted them, or will be recovered to an operational state within a reasonably short period.	
<b>Business Continuity Plan</b>	A process that defines exactly how, for which applications and for how long, a business plans to continue functioning after a disruptive event. The business continuity plan is usually an overarching plan that includes both operational and technology-related tasks.	
<b>Business Impact Analysis (BIA)</b>	This term is applicable across Technology Risk Management, in both information security and business continuity planning domains. An impact analysis results in the differentiation between critical and non-critical business functions. A function may be considered critical if there is an unacceptable impact to stakeholders from damage to the function. The perception of the acceptability of disruption may be modified by the cost of establishing and maintaining appropriate business or technical recovery solutions. A function may also be considered critical if dictated by law.	
<b>Business Process</b>	An end-to-end service made available to internal or external parties that usually corresponds to standard service products that the Service Provider offers to clients.	
<b>Business Resiliency</b>	The ability an organization has to quickly adapt to disruptions while maintaining continuous business operations and safeguarding people, assets and overall brand equity. Business resilience is more than disaster recovery, it includes post-disaster strategies to avoid costly downtime, the identification and resolution of vulnerabilities and the ability to maintain business operations in the face of additional, unexpected breaches.	
<b>Business Resiliency Procedure</b>	A process that defines exactly how, for which applications, and for how long a business plans to continue functioning after a disruptive event. The business resiliency procedure is usually an overarching procedure that includes both operational and technology-related tasks.	
<b>Change Control</b>	Also known as Change Management - The broad processes for managing organizational change. Change management encompasses planning, oversight or governance, project management, testing, and implementation. The purpose is to ensure that no unnecessary changes are made, that all changes are documented, that services are not unnecessarily disrupted and that resources are used efficiently.	FFIEC Operations Booklet and WhatIS.com

Term	Definition	Source
<b>Change Initiation Request (CIR)</b>	A document (physical or electronic) used to track change requests, including new features, enhancement requests, defects, and changed requirements. The change initiation request document must contain: <ul style="list-style-type: none"> <li>- The name of the person initiating the change</li> <li>- The system affected by the change</li> <li>- A description of the change, including the file name(s) and file location(s)</li> <li>- The date the change will occur</li> <li>- An approval signature by someone other than the person initiating the change</li> <li>- An approval date</li> </ul>	
<b>Cipher Lock</b>	A cipher lock is opened with a programmable keypad. The purpose of cipher locks is to control access, limiting either unannounced intrusions or unescorted entry to particular areas of a facility that are sensitive. A cipher lock may have four or five pushbuttons, depending on the manufacturer. Even with five pushbuttons, the code may be one to five digits. When the cipher lock unit is set up the code is programmed and shared with authorized personnel.	<a href="http://www.wisegeek.com/what-is-a-cipher-lock.htm">http://www.wisegeek.com/what-is-a-cipher-lock.htm</a>
<b>Clean Room</b>	A network segment or subnet where data is sanitized for mobile devices access only.	
<b>Client</b>	A client is the individual and/or entity for whom services are being provided by the organization.	
<b>Client Scoped Privacy Data</b>	Data received from the organization's client that includes EU "sensitive personal data" (health, religion, criminal records, trade union membership, sexual orientation and race) and in the US, protected scoped privacy data includes name, address or telephone number in conjunction with Social Security number, driver's license number, account number, credit or debit card number, personal identification number or user ID or password.	
<b>Climate Control System</b>	A combination of sensors and equipment that monitors the temperature and humidity in a sensitive environment (such as a data center) and that automatically heats/cools/dehumidifies as needed to keep the atmosphere within acceptable tolerances.	
<b>Closed Circuit TV (CCTV)</b>	CCTV is a TV system in which signals are not publicly distributed but are monitored, primarily for surveillance and security purposes. CCTV relies on strategic placement of cameras and private observation of the camera's input on monitors.	WhatIs.com
<b>Cloud Computing - NIST Definition</b>	Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This Cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.	
<b>Cloud Computing - NIST Definition of Deployment Models - Community Cloud</b>	The Cloud infrastructure is shared by several respondents and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the respondent or subcontractor and may exist on premise or off premise.	
<b>Cloud Computing - NIST Definition of Deployment Models - Hybrid Cloud</b>	The Cloud infrastructure is a composition of two or more Clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., Cloud bursting for load balancing between Clouds).	
<b>Cloud Computing - NIST Definition of Deployment Models - Private Cloud</b>	The Cloud infrastructure is operated solely for the respondent. It may be managed by the organization or a third party and may exist on premise or off premise.	
<b>Cloud Computing - NIST Definition of Deployment Models - Public Cloud</b>	The Cloud infrastructure is made available to the general public or a large industry group and is owned by the Respondent selling Cloud services.	
<b>Cloud Computing - NIST Definition of Essential Characteristics - Broad Access Network</b>	Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).	
<b>Cloud Computing - NIST Definition of Essential Characteristics - Measured Service</b>	Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.	

Term	Definition	Source
<b>Cloud Computing - NIST Definition of Essential Characteristics - On-Demand Self-Service</b>	A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.	
<b>Cloud Computing - NIST Definition of Essential Characteristics - Rapid Elasticity</b>	Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.	
<b>Cloud Computing - NIST Definition of Essential Characteristics - Resource Pooling</b>	The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.	
<b>Cloud Computing - NIST Definition of Service Models - Cloud Infrastructure as a Service (IaaS)</b>	The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying Cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).	
<b>Cloud Computing - NIST Definition of Service Models - Cloud Platform as a Service (PaaS)</b>	The capability provided to the consumer is to deploy onto the Cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying Cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.	
<b>Cloud Computing - NIST Definition of Service Models - Cloud Software as a Service (SaaS)</b>	The capability provided to the consumer is to use the provider's applications running on a Cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying Cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application.	
<b>Cloud Service Provider (CSP)</b>	The business or entity providing Cloud services.	
<b>Cold Site</b>	A remote facility that provides the equipment necessary for data and process restoration.	
<b>Co-Location</b>	A colocation (colo) is a data center facility in which a business can rent space for servers and other computing hardware. Typically, a colo provides the building, cooling, power, bandwidth and physical security while the customer provides servers and storage.	WhatIs.com
<b>Communications Plan</b>	A tool for communicating information on the considerations and implications of respondent business continuity to improve decision making.	
<b>Complex Password</b>	A password that combines alphabetic and non-alphabetic characters, such as special or numeric characters.	

Term	Definition	Source
<b>Confidential Information</b>	Confidential information means any information and/or documents of the client or its affiliates to which the organization has had access, whether in oral, written, graphic or machine-readable form, and includes, but is not limited to: (i) trade secrets and work product; (ii) information relating to business plans or practices, sales, pricing, financial data or marketing plans or methods; (iii) software, applications, systems and networks, including source code, object code and documentation and commentary related thereto; (iv) information relating to one or more customers of the subscriber or its affiliates, including, but not limited to, the following (collectively, "client data"): (1) personal information such as a customer's name, address, telephone number, account relationships, account numbers, account balances and account histories, (2) information concerning such customers that would be considered "nonpublic personal information" within the meaning of Title V of the Gramm-Leach Bliley Act of 1999 (Public Law 106-102, 113 Stat. 1338) and its implementing regulations, as the same may be amended from time to time and (3) information concerning such customers that is protected from disclosure by other applicable federal or state laws and regulations regarding privacy; (v) confidential information of third parties in the subscriber's or its affiliates' possession; (vi) security procedures and measures; and (vii) all other information related to the subscriber's and/or its affiliates' business(es). Except with respect to customer data, "client confidential information" does not include information that (i) is at the time of its disclosure publicly known; (ii) was rightfully known by licensor at the time of disclosure; or (iii) is lawfully received by licensor from a third party not bound by confidentiality obligations to the owner of such client confidential information.	
<b>Confidentiality</b>	The protection of sensitive information from unauthorized disclosure and sensitive facilities due to physical, technical, or electronic penetration or exploitation.	
<b>Configuration Management</b>	<p>Is the practice of handling changes systematically so that a system maintains its integrity over time. The Information Technology Infrastructure Library (ITIL) specifies the use of a Configuration management system (CMS) or Configuration management database (CMDB) as a means of achieving industry best practices for Configuration Management. CMDBs are used to track Configuration Items (CIs) and the dependencies between them, where CIs represent the things in an enterprise that are worth tracking and managing, such as but not limited to computers, software, software licenses, racks, network devices, storage, and even the components within such items.</p> <p>The benefits of a CMS/CMDB includes being able to perform functions like root cause analysis, impact analysis, change management, and current state assessment for future state strategy development.</p>	Wikipedia
<b>Constituent</b>	An active employee or contractor.	
<b>Contractor</b>	A contracted professional with expertise in a particular domain or area.	
<b>Covered Account</b>	A covered account is (1) an account primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, or (2) any other account for which there is a reasonably foreseeable risk to customers or the safety and soundness of the financial institution or creditor from identity theft. Each financial institution and creditor must periodically determine whether it offers or maintains a "covered account."	Section 114 of the FACT Act A. Red Flag Regulations and Guidelines
<b>Covered Entity</b>	(As defined by the HIPAA Rules requirement) A covered entity can be an Individual, a business and/or an agency who must comply with HIPAA rules to protect the privacy and security of health information and must provide individuals with certain rights related to their health information (i.e. Doctors, Health Insurance Companies, healthcare clearing house).	
<b>Critical third party service provider</b>	A service provider that is so vital that the incapacity or unavailability of such may have a debilitating impact on the business utilizing the service provider. Provides a product or performs a service for which there is no backup or alternate provider.	
<b>Cross Site Request Forgery (CSRF)</b>	An attack which can occur when a malicious website, email, blog, instant message (IM) or program causes a user's web browser to perform unwanted action on a trusted website. CSRF allows an attacker to access functionality in a target web application via the victim's already authenticated browser.	
<b>Cross Site Scripting (XSS)</b>	A computer-related security vulnerability typically found in website applications. This hacking technique can enable attackers to inject client-side script into web pages viewed by other users.	

Term	Definition	Source
<b>Data Controller</b>	Any person (including a public authority, agency or any other body) which alone or jointly with others determines the purposes and means of processing scoped privacy data (EU Directive).	
<b>Data Flow</b>	A flow describing and/or depicting the scoped privacy data for a given data subject for a given country or jurisdiction. The data flow defines the scoped privacy data and the protected scoped privacy data collected, stored, used, accessed, shared and transferred across borders of the country or jurisdiction that are secured, retained and retired.	
<b>Data segmentation and separation</b>	(see also Network Segmentation ) Better security can be achieved by not mixing trusted and untrusted applications, data, and networks. Segmentation on a cloud-computing infrastructure must provide an equivalent level of isolation as that achievable through physical network separation. Mechanisms to ensure appropriate isolation may be required at the network, operating system, and application layers; and most importantly, there should be guaranteed isolation of data that is stored.	PCI_DSS_v2_Cloud_Guidelines
<b>Data Subject</b>	Any person who can be identified, directly or indirectly, by information that identifies one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity. In certain countries (such as Austria, Luxembourg and Italy), this also includes information concerning legal entities/corporations.	
<b>Data Subject Category</b>	Includes, for example, employees, clients, business partners, customers or users.	
<b>Demilitarized Zone (DMZ)</b>	A controlled network space, delimited by firewalls or other policy-enforcing devices, which is neither inside an organization's network nor directly part of the Internet. A DMZ is typically used to isolate the respondent's most highly secured information assets while allowing predefined access to those assets that must provide or receive data outside of the respondent. The access and services provided should be restricted to the absolute minimum required.	
<b>Disaster Recovery</b>	The process, policies and procedures related to preparing for recovery or continuation of technology infrastructure critical to the respondent after a natural or human-induced disaster. Disaster recovery is a subset of business continuity	
<b>Electronic Health Records</b>	An Electronic Health Record (EHR) is an electronic version of a patient's medical history, that is maintained by the provider over time, and may include all of the key administrative clinical data relevant to that person's care under a particular provider, including demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data and radiology reports. The EHR automates access to information and has the potential to streamline the clinician's workflow. The EHR also has the ability to support other care-related activities directly or indirectly through various interfaces, including evidence-based decision support, quality management, and outcomes reporting.	<a href="https://www.cms.gov/Medicare/E-health/EHealthRecords/index.html">https://www.cms.gov/Medicare/E-health/EHealthRecords/index.html</a>
<b>Electronic System</b>	The combination of hardware and software used to manage electronic information. A system which stores information from internal and external sources to facilitate better decision making.	<a href="http://thelawdictionary.org/electronic-information-system/">http://thelawdictionary.org/electronic-information-system/</a>
<b>Emergency Periods</b>	Duration of time when a client's service provider is experiencing an emergency event that has an impact on the client.	
<b>Enclosed</b>	Closed in, surrounded, or included within.	
<b>Encryption</b>	The process of taking an unencrypted message (plaintext), applying a mathematical function to it (encryption algorithm with a key) and producing an encrypted message (ciphertext). Use of encryption protects information between the encryption process and the decryption process (the inverse of encryption) against unauthorized disclosure	ISACA CSX Fundamentals and pci_dss_glossary_v1-1
<b>Enterprise Risk Governance Program</b>	A program implemented, reviewed and maintained by an organization's Executive Board (if applicable) and Senior Management to govern the relevant factors of risks to the organization. This risk factors can include but are not limited to the following: Strategic Risks Financial Risks Operational Risks IT and Infrastructure Risks	



Term	Definition	Source
<b>Event</b>	Any detectable or discernible occurrence that has significance for the management of the IT Infrastructure or the delivery of IT service and evaluation of the impact a deviation might cause to the services. Events are typically notifications created by an IT service, Configuration Item (CI) or monitoring tool.	Wikipedia
<b>Exception</b>	A result that deviates from the norm or expectation.	
<b>Exclusion</b>	An item not fully covered by the question.	
<b>External Parties</b>	Any entity other than the organization providing responses to the SIG. Examples include (but are not limited to) service providers, contractors/consultants, vendors, etc.	
<b>External Vulnerability Scan</b>	A systematic review process executed from a network address outside of the Scoped Systems and Data network that uses software tools designed to search for and map systems for weaknesses in an application, computer or network. The intent is to determine if there are points of weakness in the security control system that can be exploited from outside the network.	
<b>Externally Facing</b>	The network entry point that receives inbound traffic.	
<b>Extranet</b>	An intranet that is partially accessible to authorized outsiders.	
<b>Facility</b>	A structure or building, or multiple structures or buildings, in which operations are conducted for the services provided. These operations include handling, processing and storage of information, data or systems, as well as personnel that support the operations.	
<b>Fire Suppression System</b>	A combination of sensors and equipment designed to detect the presence of heat/smoke/fire and actuate a fire retardant or fire extinguishing system.	
<b>Firewall</b>	A set of related programs, located at a network gateway server, that protects the resources of private networks from other networks. Firewalls may be application/proxy, packet-filtering, or stateful-based. Examples of firewalls are Cisco PIX, Check Point Firewall, Juniper NetScreen and Cyberguard. (Though they contain some firewall functionality, routers are not included in this definition.)	
<b>Firewall Rule</b>	Information added to the firewall configuration to define the respondent's security policy through conditional statements that tell the firewall how to react in a particular situation.	
<b>Fluid Sensor</b>	A mechanical device that is sensitive to the presence of water or moisture that transmits a signal to a measuring or control instrument.	
<b>Gateway</b>	A node on a network that facilitates the communication of information between two or more nodes.	
<b>General Perimeter</b>	An area with fully enclosed walls that extend from floor to ceiling (beyond raised floors and ceilings) surrounding the secure perimeter. This may be the same floor as the secure perimeter, if shared by other tenants in the facility, or the facility itself.	
<b>Generator</b>	A device that converts mechanical energy to electrical energy via an engine (usually fuel-powered) that provides electrical current as input to a power source.	
<b>Hardware Systems</b>	Includes servers and network devices.	
<b>Heat Detector</b>	A mechanical device that is sensitive to temperature and transmits a signal to a measuring or control instrument.	
<b>HIPAA</b>	Acronym that stands for the Health Insurance Portability and Accountability Act, a US law designed to provide privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals and other health care providers. The HIPAA Privacy Rule pertains to all Protected Health Information (PHI) including paper and electronic and the Security Rule deals specifically with Electronic Protected Health Information (E PHI). The Security Rule lays out three types of security safeguards required for compliance: administrative, physical, and technical.	<a href="http://www.medicinenet.com/script/main/art.asp?articlekey=31785">http://www.medicinenet.com/script/main/art.asp?articlekey=31785</a> and Wikipedia
<b>HITECH</b>	Health Information Technology for Economic and Clinical Health Act was enacted to promote the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules.	<a href="http://www.hhs.gov/hipaa-for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/index.html">http://www.hhs.gov/hipaa-for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/index.html</a>
<b>Hot Site</b>	A duplicate of the respondent's original site, with full computer systems and near-complete backups of user data.	
<b>HVAC</b>	HVAC (heating, ventilating/ventilation, and air conditioning) is the technology of indoor and vehicular environmental comfort. Its goal is to provide thermal comfort and acceptable indoor air quality.	Wikipedia

Term	Definition	Source
<b>Hypervisor</b>	A piece of software that provides abstraction of all physical resources (such as central processing units, memory, network, and storage) and thus enables multiple computing stacks (consisting of an operating system, middleware and application programs) called virtual machines to be run on a single physical host.	NIST SP 800-125B
<b>Hypervisor Console</b>	A control panel for a virtual machine manager (hypervisor) which allows multiple operating systems to share a single hardware processor.	
<b>Immediate Perimeter</b>	A rack or cage that houses the Scoped Systems and Data.	
<b>Incident</b>	Events outside normal operations that disrupt normal operational processes. An incident can be a relatively minor event, such as running out of disk space on a server, or a major disruption, such as a breach of database security and the loss of private and confidential customer information.	
<b>Incident Management</b>	A term describing the activities of an organization to identify, analyze, and correct hazards to prevent a future re-occurrence. These incidents within a structured organization are normally dealt with by either an Incident Response Team (IRT), or an Incident Management Team (IMT). These are often designated before hand, or during the event and are placed in control of the organization whilst the incident is dealt with, to restore normal functions.	Wikipedia
<b>Incident Severity</b>	A ranking of an event's significance that uses, at a minimum, a three-point scale: minor, moderately severe, and severe. For each level of severity, the respondent's IT department should define acceptable resolution times, escalation procedures, and reporting procedures.	
<b>Information Assets</b>	Scoped target and/or system data utilized/owned by an organization.	
<b>Information Security</b>	Sometimes shortened to InfoSec, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical). An information security program should include all aspects of the sensitivity of corporate information, including confidentiality, integrity and availability.	Wikipedia
<b>Information Security Review</b>	An information security assessment is a measurement of the security posture of a system or organization. The security posture is the way information security is implemented. Security assessments are risk-based assessments, due to their focus on vulnerabilities and impact. Security assessments rely on assessment methods that can accurately assess the Technology, People, and Process elements of security.	Scoping Security Assessments - A Project Management Approach (SANS Institute Reading Room site - SANS Institute May 2011)
<b>Intermediate Distribution Frame IDF</b>	A free-standing or wall-mounted rack for managing and interconnecting the telecommunications cable between end user devices and a main distribution frame (MDF).	
<b>Internal Vulnerability Scan</b>	A systematic review process using software tools designed to search for and map systems for weaknesses in an application, computer or network, executed from a network address within the Scoped Systems and Data network. Internal vulnerability scans are used to determine whether points of weakness in the security control system exist that could be exploited by a user with access to the internal network.	
<b>Internet</b>	A global network connecting millions of computers. More than 100 countries are linked into exchanges of data, news and opinions.	
<b>Internet Protocol (IP)</b>	A networking standard that allows messages to be sent back and forth over the Internet or other IP networks.	
<b>Intranet</b>	An IP network that resides behind a firewall and is accessible only to people who are members of the same organization.	
<b>Intrusion Detection Systems (IDS)</b>	A security inspection system for computers and networks that can allow for the inspection of systems activity and inbound/outbound network activity. The IDS key function identifies suspicious activity or patterns that may indicate a network or system attack.	
<b>Intrusion Protection System (IPS)</b>	A more sophisticated Intrusion Detection System (IDS) that allows administrators to configure predefined actions to be taken if suspicious activity is detected.	
<b>Inventory</b>	An itemized list of current assets.	
<b>Local Backup</b>	A method for backing up data on the local system. For example, an attached tape or storage device.	
<b>Main Distribution Frame</b>	A wiring rack that connects outside lines with internal lines. Main distribution frames are used to connect public or private lines entering the building to the respondent's internal networks	

Term	Definition	Source
<b>Malware</b>	Is designed to secretly access a computer system without the owner's informed consent. The expression is a general term (short for malicious software) used to mean a variety of forms of hostile, intrusive, or annoying software or program code. Malware includes computer viruses, worms, Trojan horses, spyware, dishonest adware, ransomware, crimeware, most rootkits, and other malicious and unwanted software or programs.	<a href="http://ithandbook.ffiec.gov/glossary.aspx">http://ithandbook.ffiec.gov/glossary.aspx</a>
<b>Man-trap</b>	Two sets of doors whereby access to the second is not granted until the individual has passed through (and closed) the first, often referred to as a "man trap." A controlled turnstile is also considered an anti-tailgating/piggybacking mechanism.	
<b>Map of Dependencies</b>	A diagram that illustrates how a business process relates to its supporting capabilities. ("Supporting capabilities" include: people involved in the delivery of the business process, application software, middleware software, servers, storage, networking, physical facilities, and people involved in the IT and physical infrastructure management.)	
<b>Master Change Log</b>	A document or database that contains a report of each change initiation request (CIR) (approved or rejected). The document or database must contain: <ul style="list-style-type: none"> <li>- Reference to a CIR</li> <li>- Date submitted</li> <li>- Date of change</li> <li>- Name of affected system</li> <li>- Approval status (approved or rejected)</li> </ul>	
<b>MD5</b>	A one-way cryptographic hash algorithm that produces a unique 128-bit alphanumeric fingerprint of its input.	
<b>Media</b>	Physical objects that store data, such as paper, hard disk drives, tapes, and compact disks (CDs).	<a href="http://ithandbook.ffiec.gov/glossary.aspx">http://ithandbook.ffiec.gov/glossary.aspx</a>
<b>Mobile Code</b>	Physical objects that store data, such as paper, hard disk drives, tapes, and compact disks (CDs).	
<b>Mobile Device</b>	smartphones, tablet computers, laptops; anyng that is not affixed to a desk or operates wirelessly	
<b>Mobile Device Management Solution</b>	Mobile device management (MDM) is an industry term for the administration of mobile devices, such as smartphones, tablet computers, laptops and desktop computers. MDM is usually implemented with the use of a third party product that has management features for particular vendors of mobile devices. It can incorporate safeguards related to but not limited to password controls, remote wipe, remote lock, detection of jailbreak devices, encryption validation.	
<b>Mobile Device Policy</b>	Policy implemented which governs the use of Mobile devices whether they be BYOD or corporate issued. This policy can incorporate details related to Security training, Terms of Use, constituent responsibilities, data handling and access controls.	
<b>Modem</b>	A device that allows a computer or terminal to transmit data over an analog telephone line.	
<b>Multi-factor Authentication</b>	Multifactor authentication requires the use of solutions from two or more of the three categories of factors: <ul style="list-style-type: none"> <li>• Something the user knows (e.g., password, PIN).</li> <li>• Something the user has (e.g., ATM card, smart card).</li> <li>• Something the user is (e.g., biometric characteristic, such as a fingerprint).</li> </ul> Using multiple solutions from the same category at different points in the process may be part of a layered security or other compensating control approach, but it would not constitute multifactor authentication.	
<b>N+1</b>	N+1 redundancy is a form of resilience that ensures system availability in the event of component failure. Components (N) have at least one independent backup component (+1).	Wikipedia
<b>Network Address Translation (NAT)</b>	A process of rewriting the source and/or destination addresses of IP packets as they pass through a network device.	
<b>Network Devices</b>	Units that mediate data in a computer network. Computer networking devices are also called network equipment, Intermediate Systems (IS) or InterWorking Unit (IWU).	
<b>Network Segment</b>	A portion of a computer network that is separated from the remainder of the network by a device such as a repeater, hub, bridge, switch or router. Each segment may contain one or multiple computers or other hosts. Network segments are typically established for throughput and/or security reasons.	

Term	Definition	Source
<b>Network time protocol (NTP)</b>	A protocol designed to synchronize the clocks of computers over a network.	
<b>Node</b>	Any physical device with a unique network address.	
<b>Non-Employees</b>	Auditors, consultants, contractors, and vendors.	
<b>Non-Public Information (NPI)</b>	Any personally identifiable or company proprietary information that is not publicly available. Non-public information includes but is not limited to: certain company proprietary information, such as internal policies and memorandums; and personal information such as an individual's name, address or telephone number. It also includes information requiring higher levels of protection according to the company's security policy, such as company proprietary trade secrets or personal information that bundles an individual's name, address or telephone number with a Social Security number, driver's license number, account number, credit or debit card number, personal identification number, health information, religious opinions or a user ID or password.	
<b>Non-Public Personal Information (NPPI)</b>	Any personally identifiable information that is not publicly available. Non-public, personal information includes but is not limited to name, address, city, state, zip code, telephone number, Social Security number, credit card number, bank account number and financial history.	
<b>Notice Consent Language</b>	Any data subject consent language in a privacy notice to be accepted by a data subject (expressly or by implication). The language may relate to consent to the entire privacy notice or to particular uses of the scoped privacy data where a data subject's non-consent to this use of the scoped privacy data results in a data subject rejecting the privacy notice. Examples of uses include cross-border transfer of scoped privacy data, special use of the scoped privacy data or special local regulatory requirements.	
<b>Open Web Application Security Project (OWASP)</b>	An open, online community dedicated to enabling organizations to conceive, develop, acquire, operate and maintain web applications that can be trusted.	
<b>Owner</b>	An individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. Ownership is not an indication of property rights to the asset.	
<b>Ownership</b>	A formally assigned responsibility for a given asset.	
<b>Penetration Testing</b>	A conventional security control and the one most widely used by software vendors.	
<b>Permission</b>	Any data subject permission (opt in or opt out) required to use or share scoped privacy data that can be easily switched on and off, including for the following purposes: marketing, affiliate sharing, product use, promotions, newsletters, tailoring services to data subject's particular requirements, behavioral and purchasing patterns, social networking and professional networking, excluding notice consent language.	
<b>Personal Health Records</b>	A personal health record ( PHR ) is an electronic application used by patients to maintain and manage their health information in a private, secure, and confidential environment. PHRs are managed by patients.	<a href="https://www.healthit.gov/providers-professionals/faqs/what-personal-health-record">https://www.healthit.gov/providers-professionals/faqs/what-personal-health-record</a>
<b>Personal Identification Number (PIN)</b>	A secret shared between a user and a system that can be used to authenticate the user to the system.	
<b>Personally Identifiable Informatin (PII)</b>	NIST Special Publication 800-122 defines PII as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."	Wikipedia and NIST 800-122
<b>Physical Media</b>	Any portable device or substance (e.g., paper) used to store data for specific and legitimate purposes. Examples of physical media include: <ul style="list-style-type: none"> <li>- Magnetic tapes and disks</li> <li>- Cartridges, including 9-track, DAT, and VHS</li> <li>- Optical disks in CD and DVD format</li> <li>- Microfilm/fiche</li> <li>- Paper (e.g., computer-generated reports and other printouts)</li> <li>- Static memory devices, such as USB memory sticks</li> </ul>	
<b>Port Scan</b>	A systematic scan of a computer's ports that identifies open doors. Used in managing networks, port scanning also can be used maliciously to find a weakened access point from which to break into computer.	

Term	Definition	Source
<b>Post-Deployment Test Document</b>	<p>A document that provides evidence that the change was tested and approved in the production environment. The document must contain:</p> <ul style="list-style-type: none"> <li>- Reference to a CIR</li> <li>- Identified deployment resources</li> <li>- Deployment start date</li> <li>- Deployment end date</li> <li>- Expected results</li> <li>- Actual results</li> <li>- Approval signature</li> <li>- Approval date</li> </ul>	
<b>Potential Access</b>	<p>Under ordinary circumstances, individuals that are not permitted access to Scoped Data are, however, in certain circumstances able or are permitted access to Scoped Data. For example: a senior executive who reviews Scoped Data in the course of an investigation, or a courier and truck driver who picks up documents in a locked shred bin and transports them in the locked shred bin to a warehouse for shredding.</p>	
<b>Power Redundancy</b>	<p>Any type of power delivery mechanism that provides continuous power to connected systems in the event of a failure in the main delivery mechanism for electricity. Such mechanisms include multiple electric feeds, automatic failover generators, and uninterruptible power supplies.</p>	
<b>Pre-Deployment Test Document</b>	<p>A document (electronic or paper) that provides evidence that the requested changes were tested prior to deployment in the production environment. A pre-deployment test document is inspected for:</p> <ul style="list-style-type: none"> <li>- Reference to a CIR</li> <li>- Identified testing resources</li> <li>- Testing start date</li> <li>- Testing end date</li> <li>- Expected test results</li> <li>- Actual test results</li> </ul>	
<b>Privacy Incident</b>	<p>A privacy incident is the unauthorized collection, use, access, retention or disclosure of personal or otherwise sensitive information.</p>	
<b>Privacy Inventory Flow</b>	<p>The current scoped privacy data inventory/list and flow by data subject category that has been approved by management of the organization. A privacy inventory flow identifies the ownership of the scoped privacy data, its sources, collection methods, storage locations, uses (by who, where and for what purpose), sharing within the organization and among its third parties, trans-border flows and adequacy mechanisms chosen to ensure the protection of such scoped privacy data, security, retention and deletion schedules and mechanisms.</p>	
<b>Privacy Notice</b>	<p>Notice given to data subjects on the collection, use, storage, sharing, transfer, retention and destruction of their scoped privacy data in accordance with privacy applicable law and organization policy.</p>	
<b>Privacy Policy</b>	<p>An organization's internal policy adopted for the life cycle of the scoped privacy data.</p>	
<b>Privacy Risk Assessment</b>	<p>A privacy risk/impact assessment states what personally identifiable information (PII) is collected and explains how that information is maintained, how it will be protected and how it will be shared.</p> <p>A PIA should identify:</p> <ul style="list-style-type: none"> <li>- Whether the information being collected complies with privacy-related legal and regulatory compliance requirements.</li> <li>- The risks and effects of collecting, maintaining and disseminating PII.</li> <li>- Protections and processes for handling information to alleviate any potential privacy risks.</li> <li>- Options and methods for individuals to provide consent for the collection of their PII.</li> </ul> <p>Generally Accepted Privacy Principles (GAPP) is a recognized framework for assessing privacy risk. GAPP operationalizes complex privacy requirements into a single privacy objective that is supported by 10 privacy principles.</p>	<p><a href="http://searchcompliance.techtarget.com/definition/Privacy-impact-assessment-PIA">http://searchcompliance.techtarget.com/definition/Privacy-impact-assessment-PIA</a> and <a href="http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/DownloadableDocuments/10261378ExecOverviewGAPP.pdf">http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/DownloadableDocuments/10261378ExecOverviewGAPP.pdf</a></p>

Term	Definition	Source
<b>Privileged Access</b>	This access grants an employee access to more than usual company data or make changes to the company network. Companies need privileged users because they have access to source code, file systems and other assets that allow them to upgrade the systems or make other technical changes.	2016 AUP Glossary
<b>Protected Health Information (PHI)</b>	The Privacy Rule protects individually identifiable health information, called PHI, held or transmitted by a covered entity or its business associate, in any form, whether electronic, paper, or verbal. PHI includes information that relates to all of the following: <input type="checkbox"/> The individual's past, present, or future physical or mental health or condition - The provision of health care to the individual <input type="checkbox"/> The past, present, or future payment for the provision of health care to the individual PHI includes many common identifiers, such as name, address, birth date, and Social Security number.	HIPAA BASICS FOR PROVIDERS: PRIVACY, SECURITY, AND BREACH NOTIFICATION RULES
<b>Protected Scoped data</b>	Scoped data or any other data that requires a higher level of protection or special treatment due to its sensitivity under: security applicable law; company security policy; and/or as identified in the scope definition of protected scoped data of the Shared Assessments Standardized Information Gathering (SIG) questionnaire and Shared Assessments Agreed Upon Procedures (AUP), a tool for standardized onsite assessments. This may include: scoped data, such as name, address or telephone number in conjunction with Social Security number, driver's license number, account number, credit or debit card number, personal identification number, user ID or password; an individual's health information; company trade secrets or certain confidential information. Data that falls under the definitions of both scoped data and protected scoped data (for example, credit card details).	
<b>Protected Scoped Privacy data</b>	Any scoped privacy data required to have a higher level of protection or special treatment under privacy applicable law due to its sensitivity, e.g., encryption. This includes EU "sensitive personal data" (health, religion, criminal records, trade union membership, sexual orientation and race). In the US, protected scoped privacy data includes name, address or telephone number in conjunction with Social Security number, driver's license number, account number, credit or debit card number, personal identification number or user ID or password.	
<b>Protocol</b>	A set of rules and formats that enable the proper exchange of information between different systems.	
<b>Publicly Accessible</b>	In networking terms, able to accept a connection originating from the public domain, e.g., the Internet.	
<b>Quality Analysis and User Acceptance Testing (QA UAT)</b>	QA testing usually precedes UAT. QA examines the functional behavior of individual components and integrated feature-level capacity. UAT typically refers to the final testing process prior to deployment.	
<b>Raised Floor</b>	Used in data center construction, a raised floor above the "true" floor allows air conditioning flow and wiring to pass freely under equipment. The space between the true and raised floors is accessed by removable floor tiles.	
<b>Receiver Company</b>	The organization that has contracted with a service provider for a specific service.	
<b>Recovery Time Objective (RTO)</b>	The targeted duration of time and a service level for which a business process must be restored after a disaster or disruption of service, in order to avoid unacceptable consequences, should a break occur in business continuity.	
<b>Red Flag</b>	The Red Flags Rule requires many businesses and organizations to implement a written identity theft prevention program designed to detect the "red flags" of identity theft in their day-to-day operations, take steps to prevent the crime, and mitigate its damage. A program can help businesses spot suspicious patterns and prevent the costly consequences of identity theft. The Federal Trade Commission (FTC) enforces the Red Flags Rule with several other agencies. "Red Flags Rule" is formally known as the "Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003; Final Rule". The rule applies only to federally regulated financial institutions, and through the FTC, to certain creditors. The term Covered Accounts is contained in the rule.	ftc.gov and Web Hull
<b>Remediation</b>	The process by which organizations address information systems control deficiencies and maturity gaps to ensure that deficiencies are appropriately corrected.	
<b>Remote Access</b>	Remote access refers to the ability to access a computer, such as a home computer or an office network computer, from a remote location. This allows employees to work offsite, such as at home or in another location, while still having access to a distant computer or network, such as the office network.	Technopedia

Term	Definition	Source
<b>Removable Device</b>	Removable devices are any type of storage device that can be removed from a computer while the system is running. Examples of removable media include CDs, DVDs and Blu-Ray disks, as well as diskettes and USB drives.	
<b>Residual Risk Rating Scoring Method</b>	A calculation of the risk that remains after security controls have been applied.	
<b>Risk Assessment</b>	The process of identifying variables that have the potential to negatively impact an organization's ability to conduct business. A prioritization of potential business disruptions based on severity and likelihood of occurrence. The risk assessment includes an analysis of threats based on the impact to the institution, its customers, and financial markets, rather than the nature of the threat.	TechTarget and FFIEC IT Examination Handbook Glossary
<b>Risk Governance</b>	Governance refers to the actions, processes, traditions and institutions by which authority is exercised and decisions are taken and implemented. Risk governance applies the principles of good governance to the identification, assessment, management and communication of risks Effective risk governance should provide the operating model and decision-making framework needed to identify and respond to risks.	<a href="https://www.irgc.org/risk-governance/what-is-risk-governance/">https://www.irgc.org/risk-governance/what-is-risk-governance/</a>
<b>Risk Prioritization Scoring Method</b>	A systematic approach that quantifies risk in terms of loss potential, then sequences individual risks to determine the order in which compensating controls should be implemented.	
<b>Risk Scenario</b>	An IT risk scenario is a description of an IT related event that can lead to a business impact, when and if it should occur. A risk scenario is characterized by: - a threat actor - a threat type - event - asset or resource affected - time The risk scenario structure differentiates between loss events (events generating the negative impact), vulnerabilities or vulnerability events (events contributing to the magnitude or frequency of loss events occurring), and threat events (circumstances or events that can trigger loss events).	Wikipedia
<b>Role-Based User Access</b>	Role-based access control (RBAC) is a method of regulating access to computer or network resources based on the roles of individual users within an enterprise. Roles are defined according to job competency, authority and responsibility within the enterprise.	
<b>Root cause analysis</b>	A root cause is a factor that caused a nonconformance and should be permanently eliminated through process improvement. Root Cause Analysis (RCA) describes a wide range of approaches, tools, and techniques used to uncover causes of problems. RCA is based on the basic idea that effective management requires more than merely "putting out fires" for problems that develop, but finding a way to prevent them.	ASQ.org
<b>Safe Harbor</b>	Intended for U.S. organizations that process personal data collected in the EU, the Safe Harbor Principles are designed to assist eligible organizations to comply with the EU Data Protection Directive and maintain the privacy and integrity of that data. NOTE: The EU Privacy Shield program is the successor of the EU US Safe Harbor program. Announced in Feb 2016 it became operational on the 1st August 2016	<a href="https://www.privacytrust.com/guidance/safe_harbor.html">https://www.privacytrust.com/guidance/safe_harbor.html</a>
<b>Sanctions Check</b>	In most countries, organizations are prohibited by law from doing business with drugs and arms merchants and terrorist organizations. Sanctions lists ranging from OFAC to the EU Consolidated Lists to the Interpol Most Wanted to the Hong Kong and Singapore Monetary Authority exist. Part of due diligence in vendor selection should include screening of the third party against sanctions lists.	should this be removed from the questionnaire? P.3.5
<b>Scoped Data</b>	A client's non-public personal information (NPPI), protected health information (PHI), personal information (PI) or non-public information that is stored, transmitted or processed by the service provider. Scoped data may also include any data selected as being in scope by the organization or client at the scoping of the engagement. Any reference to scoped data includes protected scoped data, where applicable.	

Term	Definition	Source
<b>Scoped Privacy Data</b>	Any information relating to a data subject, who can be identified directly or indirectly, by that information, and in particular, by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity. Examples of scoped privacy data include name, address, telephone number and email address. Scoped privacy data may exist in any media or format. Any reference to scoped privacy data includes protected scoped privacy data, where applicable.	
<b>Scoped Systems and Data</b>	Computer hardware, software and/or Non-Public Personal Information that is stored, transmitted, or processed by the service provider in scope for the engagement.	
<b>Scoping Meeting</b>	A meeting held prior to commencement of a Shared Assessments engagement, to determine the Scoped Systems and Data to be included in a company's Standardized Information Gathering Questionnaire (SIG) and Agreed Upon Procedures (AUP) assessment.	
<b>Secure Code Review</b>	The process of identifying whether software code meets the respondent's security requirements.	
<b>Secure Perimeter</b>	A space fully enclosed by walls that surround the immediate perimeter and that extend from floor to ceiling (beyond raised floors and ceilings), which is contained, and whose points of entry are secured.	
<b>Secure Socket Layer (SSL)</b>	A protocol developed by Netscape for transmitting private documents via the Internet. SSL uses a cryptographic system with two keys to encrypt data: a public key known to everyone and a private or secret key known only to the recipient of the message.	
<b>Secure Workspace</b>	An environment from where people work from their desks with the purpose of accessing, editing or inputting Scoped Systems and Data on a computer, telephone or physical media, e.g., a BPO or call center environment.	
<b>Secure Workspace Perimeter</b>	A space fully enclosed by walls that surround the Secure Workspace which is contained, and whose points of entry and exit are secured.	
<b>Security Applicable Law</b>	Applicable laws, enactments, regulations, binding industry codes, regulatory permits and licenses which are in effect that address the protection, handling and security of scoped data and protected scoped data and that are determined to be in scope by the organization or client at the scoping of the engagement.	
<b>Security Architecture Risk Analysis</b>	Defines concepts, methods, and techniques for analyzing the architecture and design of software systems for security flaws.	
<b>Security Policy</b>	A published document or set of documents defining requirements for one or more aspects of information security.	
<b>Segmentation / Separation (of data)</b>	see Data Segmentation / Separation	
<b>Sensitive customer financial information</b>	A customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. Sensitive customer information also includes any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name and password or password and account number.	Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice
<b>Sensitive Information</b>	Also known as "scoped data," any customer data stored at the organization's facility. This data may be stored in the form of physical media, digital media or any other storage medium.	
<b>Server</b>	A computer that makes services, such as access to data files, programs, and peripheral devices, available to workstations on a network.	
<b>Service Account</b>	A service account is a user account that has been created to run a particular piece of software or service. The account belongs to the software application instead of to an individual end user.	
<b>Service Level Agreement (SLA)</b>	An agreement that details the responsibilities of an IT service provider, the rights of the service provider's customers, and the penalties assessed when the service provider violates any element of the SLA. SLAs also identify and define the service, plus the supported products, evaluation criteria, and quality of service customers should expect. SLAs are typically measured in terms of metrics. Examples include processing completion times and systems availability times.	FFIEC IT Examination Handbook Glossary
<b>Service Provider</b>	An subcontractor that provides outsourced services, such as data processing, business operations, applications, systems or staffing.	
<b>Service Set Identifier (SSID)</b>	A 32-character unique identifier attached to the header of packets sent over a wide area network to identify each packet as part of that network.	



Term	Definition	Source
<b>Simple Mail Transfer Protocol (SMTP)</b>	The de facto standard for email transmissions across the Internet.	
<b>Smoke Detector</b>	A mechanical device that is sensitive to the presence of smoke or particulate material in the air that transmits a signal to a measuring or control instrument.	
<b>Software</b>	Vendor developed software code used for custom or commercial-off-the-shelf purposes.	
<b>Software Architecture</b>	The process of defining a structured software solution that meets all of the technical and operational requirements, while optimizing common quality attributes such as performance, security, and manageability.	
<b>Software Security Group</b>	A group whose charter is to assist in the design, review and implementation of software that protects the information and resources contained in and controlled by that software.	
<b>Status Change</b>	Change to employment status that is recorded by human resources, such as promotions, demotions or departmental changes.	
<b>Stewardship</b>	The act of managing and maintaining a given asset.	
<b>Storage Facility</b>	The physical location where target systems and data are stored.	
<b>Strong Password</b>	<p>Password length must be a minimum of seven (7) characters, must not to contain a common usage word or a word found in the English dictionary, may not contain user name, any part of a full name or access level of the user and must contain characters from at least three (3) of the following four (4) classes of characters:</p> <ul style="list-style-type: none"> <li>• Upper case letters (A, B, C, ....Z)</li> <li>• Lower case letters (a, b, c, ....z)</li> <li>• Numbers (0,1, 2, ...9)</li> <li>• Non-alphanumeric ("special characters") such as punctuation symbols</li> </ul>	
<b>Subcontractor</b>	is a business or an individual that signs a contract to perform part or all of the obligations of another's contract.	
<b>System Owner</b>	The business unit that retains financial ownership or decision rights for the business use of the asset.	
<b>System Steward</b>	The primary assigned administrator responsible for maintenance and day-to-day tasks that support the business.	
<b>Systems Development Life Cycle (SDLC)</b>	A process for planning, creating, developing, testing and deploying a software application or information system.	
<b>Target System</b>	Computer hardware and software in scope for the engagement that contains scoped data.	
<b>Third Party</b>	All entities or persons that work on behalf of the organization but are not its employees, including consultants, contingent workers, clients, business partners, service providers, subcontractors, vendors, suppliers, affiliates and any other person or entity that accesses Scoped Systems and Data.	
<b>Threat Impact Calculation Method</b>	A systematic method of determining the loss potential of a particular threat, based on the value of assets affected.	
<b>Threat Modeling</b>	<p>Threat modeling allows you to systematically identify and rate the threats that are most likely to affect your system. By identifying and rating threats based on a solid understanding of the architecture and implementation of your application, you can address threats with appropriate countermeasures in a logical order, starting with the threats that present the greatest risk.</p> <p>Threat modeling has a structured approach that is far more cost efficient and effective than applying security features in a haphazard manner without knowing precisely what threats each feature is supposed to address.</p>	
<b>Threat Probability Calculation Method</b>	<p>A systematic method of determining the potential for a particular threat to occur, based on the likelihood of the occurrence collected from internal staff, past records, and official security records.</p> <p>Threats x Vulnerability x Asset Value = Total Risk  (Threats x Vulnerability x Asset Value) x Controls Gap = Residual Risk</p>	
<b>Token</b>	A unique identifier generated on both a host and small, user-held device that allows the user to authenticate to the host.	
<b>Transmission Control Protocol (TCP)</b>	A protocol of TCP/IP networks. TCP, the basic communication language (or protocol) of the Internet, enables two hosts to establish a connection and exchange streams of data.	
<b>True Ceiling</b>	The permanent overhead interior surface of a room, constructed of solid building materials offering resistance to and evidence of unauthorized entry.	
<b>True Floor</b>	The permanent bottom interior surface of a room, constructed of solid building materials offering resistance to and evidence of unauthorized entry.	

Term	Definition	Source
<b>Two-factor Authentication</b>	(aka multi-factor authentication ) The process of using two or more factors to achieve authentication. Factors include something you know (e.g., password or personal identification number); something you have (e.g., cryptographic identification device or token); and something you are (e.g., biometric).	FFIEC_CAT_App_C_Glossary_June_2015_PDF5
<b>UI</b>	In information technology, the user interface (UI) is everything designed into an information device with which a human being may interact -- including display screen, keyboard, mouse, light pen, the appearance of a desktop, illuminated characters, help messages, and how an application program or a Web site invites interaction and responds to it.	TechTarget
<b>Unapproved</b>	Operating without consent.	
<b>Unidentified</b>	Being or having an unknown or unnamed source.	
<b>Uninterruptible Power Supply (UPS)</b>	A power supply consisting of a bank of batteries, which is continually charged. When power fails, the UPS becomes the source of electrical current for computer equipment until the batteries are discharged. A UPS is often connected to a generator that can provide electrical power indefinitely.	
<b>User Datagram Protocol (UDP)</b>	A communications protocol within the Internet protocol suite. UDP, which uses a simple, connectionless transmission model with a minimum of protocol mechanism, performs similar functions as TCP (except datagrams are created instead of packets), but UDP lacks the flow-control and error-recovery functions, allowing for fewer system resources.	
<b>Vendor Management</b>	Vendor management is a discipline that enables organizations to control costs, drive service excellence and mitigate risks to gain increased value from their vendors throughout the deal life cycle. Vendor risk management (VRM) is a comprehensive plan for identifying and decreasing potential business uncertainties and legal liabilities regarding the hiring of 3rd party vendors for information technology (IT) products and services.	Gartner IT Glossary and TechTarget
<b>Vibration Alarm Sensor</b>	An alarm that responds to vibrations in the surface onto which it is mounted. A normally closed switch momentarily opens when the sensor is subjected to a vibration of sufficiently large amplitude.	
<b>Virtual Machine (VM)</b>	A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. The virtual machine is comprised of a set of specification and configuration files and is backed by the physical resources of a host.	vmware.com
<b>Virtual Private Network (VPN)</b>	A communication tunnel running through a shared network, such as the Internet, which uses encryption and other security mechanisms to ensure the data cannot be intercepted and that the data senders and receivers are authenticated.	
<b>Volumetric Alarm Sensor</b>	An alarm sensor designed and employed to detect an unauthorized person in a confined space when the space is normally unoccupied. Such alarms include ultrasonic, microwave, and infrared sensors.	
<b>Vulnerability</b>	A hardware, firmware, or software flaw that leaves an information system open to potential exploitation; a weakness in automated system security procedures, administrative controls, physical layout, internal controls, etc., that could be exploited to gain unauthorized access to information or to disrupt critical processing.	FFIEC IT Examination Handbook Glossary
<b>Vulnerability Management</b>	Vulnerability management is the process in which vulnerabilities in IT are identified and the risks of these vulnerabilities are evaluated. This evaluation leads to correcting the vulnerabilities and removing the risk or a formal risk acceptance by the management of an organization (e.g. in case the impact of an attack would be low or the cost of correction does not outweigh possible damages to the organization).	Implementing a vulnerability management process - SANS Institute Reading Room
<b>War Walk</b>	Also known as "war drive," using a laptop to "sniff" for wireless access points. War walking may be used to locate a public access point for personal use or as a controls assessment to identify access points that are inadequately secured and may indicate an elevated risk of breach.	
<b>Warm Site</b>	A remote facility which replicates production data in set intervals.	
<b>Water Sensor</b>	A mechanical device sensitive to the presence of water or moisture that transmits a signal to a measuring or control instrument.	
<b>Whistleblowing Policy</b>	A policy protecting anyone who has and reports insider knowledge of illegal activities occurring in an organization. Whistleblowers can be employees, suppliers, contractors, clients or any individual who somehow becomes aware of illegal activities taking place in a business, either through witnessing the behavior or being told about it.	

Term	Definition	Source
<b>Wireless Networks</b>	A wireless network, a.k.a. wireless local-area network (LAN), uses radio waves to connect devices such as laptops to the Internet and to your business network and its applications instead of physical cables like a wired network does. An example of wireless network is when you connect a laptop to a WiFi hotspot at a cafe, hotel, airport lounge or other public place you're connecting to that business's wireless network.	
<b>Workstation</b>	(1) Single-user computers typically linked together to form a local area network, that can also be used as standalone systems. (2) In networking, any computer connected to a local area network, including a workstation or personal computer.	
<b>XSS</b>	Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy.	Wikipedia

<b>Formula Notes</b>	
<b>Column</b>	<b>Description</b>
<b>A</b> <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 C22 (below).
<b>A4</b>	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>D</b> <b>Conditional Formatting</b> <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.
<b>E</b> <b>Conditional Formatting</b> <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 the top of a table question.
<b>I</b> <Q Depth>	Values in this column indicate the depth (number of decimal places) the question has.
<b>J</b> <Table ID>	A value of "1" in this cell indicate the top of a table.
<b>K</b> <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.
<b>L - O</b> <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, if 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.
<b>P</b> <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 Master (this tab, D6) is selected then high level responses are ignored.
<b>Q</b> <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".
<b>R</b> <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.
<b>S</b> <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.
<b>T</b> <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.
<b>U</b> <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.
<b>V</b> <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.
<b>W</b> <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.
<b>X</b> <HL Chk>	Identifies if the question is duplicated on the Lite tab

**If this SIG will be a Master SIG to be used with the SMT, select Master below. If this SIG will be distributed leave blank.**

Column (Cell)	Formula	Highest Ser #
A	Hard coded, unique serial number (Rows without questions have no serial numbers)	#REF!
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)	
<b>Named Range</b>	<b>Formula</b>	
Master	Formula Notes!\$D\$5	
L2_Array	Lv2_ Questions!\$A\$4:\$U\$568	
SIG_Data	Full!\$E\$3:\$H\$951	
Sheet Protection	8bd0z4XW	

Ques Num	SIG Question Text	Response	Maturity	Additional Information	AUP 2017 Relevance	ISO 27002:2013 Relevance	Appendix J Section and Line Reference	FFIEC CAT Tool_June 2015	PCI 3.2_April	FFIEC IT Mgmt	COBIT 4.1 Relevance	NIST Cybersecurity Framework_February2014	
<b>SIG Lite</b>													
<b>A. Risk Assessment and Treatment</b>													
SL.1	Is there a risk assessment program that has been approved by management, communicated to constituents and an owner to maintain and review the program? If yes, does it include:				A.1 IT & Infrastructure Risk Governance and Context	5.1 6.1.2	Leadership & Commitment, Information Security Risk Assessment	Governance: Oversight Risk Management: Risk Assessment D1.G.Ov.B.2 D1.RM.RA.B.1 D1.RM.RA.B.2	12.2	1.A.1 3.B	PO9.4	ID.GV-4 ID.RA-5 ID.RM-1	
SL.2	Is there a program to manage the treatment of risks identified during assessments?				A.2 IT & Infrastructure Risk Assessment Life Cycle	6.1.3	Information Security Risk treatment		N/A	1.A.2 2.A	PO9.4		
SL.3	A formal process for assigning appropriate management ownership for each risk?				A.2 IT & Infrastructure Risk Assessment Life Cycle					1.B.7(b) 2.A			
SL.4	A formal process for appropriate management knowingly and objectively accepting risks and approving action plans?				A.2 IT & Infrastructure Risk Assessment Life Cycle					2.A		ID.RM-2	
SL.5	A formal process for tracking the status of action plans and reporting them to management?				A.2 IT & Infrastructure Risk Assessment Life Cycle					2.A 3.D.7			
SL.6	Controls identified for each material risk?				A.2 IT & Infrastructure Risk Assessment Life Cycle					2.A			
SL.7	Measures for defining, monitoring, and reporting risk metrics?				A.2 IT & Infrastructure Risk Assessment Life Cycle					1.A.3			
SL.8	Do Subcontractors have access to Scoped Systems and Data? (backup vendors, service providers, equipment support maintenance, software maintenance vendors, data recovery vendors, etc.)? If yes, is there:					15	Supplier relationships		12.8		DS1.1, DS1.2, DS1.3, DS2.4		
SL.9	A documented vendor management process in place for the selection, oversight and risk assessment of third party vendors? If yes, does it include:				A.7 Subcontractor Selection and Management Process	15.1.1	Information security policy for supplier relationships	Relationship Management: Due Diligence	D4.RM.DD.B.2	12.8 12.8.3 12.8.4	3.C.3 3.C.5 3.C.8 12.8	DS1.5, DS2.4, ME2.6	
SL.10	Approval by management?				A.7 Subcontractor Selection and Management Process	5.1.1	Policies on information security				PO4.14, DS2.1, DS2.3, DS5.4, DS5.9, DS5.11, DS12.3		
SL.11	Annual review?				A.7 Subcontractor Selection and Management Process	5.1.2	Review of the policies for information security	Relationship Management: Ongoing Monitoring	D4.RM.OM.B.1	12.8.4	PO4.14, PO6.4, PO8.3, AI5.2, DS2.2, DS2.3, DS2.4, DS5.1, ME2.6		
SL.12	Required reassessment when service delivery or contract changes?												
SL.13	Review of the subcontractor's vendor management policy and procedures?				A.9 Documenting Information Security Assessments for Subcontractors	15.2.1.g	Monitoring and review of supplier services		N/A		DS1.5, DS2.2, DS2.3		
SL.14	Is there a process to identify and log subcontractor information security, privacy and/or data breach issues?				A.9 Documenting Information Security Assessments for Subcontractors	15.2.1.e	Monitoring and review of supplier services		N/A		DS3.1, DS3.2, DS3.3		
SL.15	Is there a vendor management program?				A.5 Vendor Risk Management Program			Relationship Management: Due Diligence	D4.RM.DD.B.2	12.8.4	3.A.1 3.C.3 3.C.5		
SL.16	Do external parties have access to Scoped Systems and Data or processing facilities?					15	Supplier relationships	Governance: Strategies & Policies	D1.G.SP.B.5	12.8	PO6.4, DS5.5, ME2.2, ME2.5, ME4.7		
SL.17	Is the maturity of IT management processes formally evaluated at least annually using an established benchmark (e.g., COBIT maturity models)?					17.1.3	Verify, review and evaluate information security continuity		N/A				
SL.18	Are there regular privacy risk assessments conducted? If yes, provide frequency and scope. If no, explain reason.				P.3 Privacy Organization and Program Maintenance	15.1.3.i	Information and communication technology supply chain		N/A				
SL.19	Are identified privacy risks and associated mitigation plans formally documented and reviewed by management?				P.3 Privacy Organization and Program Maintenance	15.1.1.1	Information security policy for supplier relationships	Risk Management: Audit Corrective Controls: Remediation	D1.RM.Au.B.4 D3.CC.R.B.1	N/A			
SL.20	Are reasonable resources (in time and money) allocated to mitigating identified privacy risks?				P.3 Privacy Organization and Program Maintenance			Corrective Controls: Remediation	D3.CC.R.B.1	N/A			
SL.21	Is there a compliance risk management system that addresses the quality and accuracy of reported consumer data?				P.3 Privacy Organization and Program Maintenance				N/A				
SL.22	Is there a compliance risk management system that addresses the quality of assembling and maintaining the data?				P.3 Privacy Organization and Program Maintenance				N/A				
<b>B. Security Policy</b>													
SL.23	Is there an information security policy that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?				B.1 Information Security Policy Maintenance	5.1.1	Policies for information security	Governance: Strategies & Policies	D1.G.SP.B.4	5.4 10.9 12.2	1.B.2 3.C.1 3.C.3(b)	PO6.1, PO6.2, PO6.3, PO6.5, DS5.2, DS5.3, ME2.1	ID.GV-1
SL.24	Have the policies been reviewed in the last 12 months?				B.1 Information Security Policy Maintenance	5.1.2	Review of the policies for information security			12.1.1	PO3.1, PO5.3, PO5.4, PO6.3, PO9.4, DS5.2, DS5.3, ME2.2, ME2.5, ME2.7, ME4.7		

Ques Num	SIG Question Text	Response	Maturity	Additional Information	AUP 2017 Relevance	ISO 27002:2013 Relevance	Appendix J Section and Line Reference	FFIEC CAT Tool_June 2015	PCI 3.2_April	FFIEC IT Mgmt	COBIT 4.1 Relevance	NIST Cybersecurity Framework_February2014
<b>C. Organizational Security</b>												
SL.25	Is there a respondent information security function responsible for security initiatives?				C.1 Security Organization Roles / Responsibilities	6.1.1	Information Security Roles and Responsibilities		12.5		PO3.3, PO3.5, PO4.3, PO4.4, PO4.5, PO4.8, PO6.3, PO6.4, PO6.5, DSS.1	
<b>D. Asset and Information Management</b>												
SL.26	Is there an asset management policy approved by management, communicated to constituents and an owner to maintain and review?				D. Asset and Information Management	8.1	Responsibility for Assets	Governance: IT Asset Management D1.G.IT.B.1 D1.G.IT.B.3	N/A	3.A.1	PO4.14, PO6.4, PO8.3, AI5.2, DS2.2, DS2.3, DS2.4, DS5.1, ME2.6	
SL.27	Is information classified?				D.1 Asset Accounting and Inventory	8.2.1	Classification of Information	Governance: IT Asset Management D1.G.IT.B.2	9.6.1		PO2, AI2, DS9	ID-AM-1 ID-AM-2
SL.28	Is there a removable media policy or program (CDs, DVDs, tapes, disk drives) that has been approved by management, communicated to appropriate constituents, and an owner to maintain and review the policy?				D.4 Removable Device Security	8.3.1	Management of Removable Media	Preventative Controls: Access and Data Management Preventative Controls: Device/End-Point Security D3.PC.ADM.B.14 D3.PC.DEPS.B.1	9.7.1		DS5.4, DSS.7	PR-PT-2
SL.29	Is Scoped Data sent or received via physical media?				D.2 Physical Media Tracking	8.3.3	Physical Media in Transit		N/A		AI6.3, DS5.7	PR-DS-5
SL.30	Are encryption tools managed and maintained for Scoped Data? If yes:				D.5 Data Security Policy - Encryption	10.1	Cryptographic controls		3.5.3 3.6.1 3.6.4 3.6.5		N/A	
SL.31	Are clients provided with the ability to generate a unique encryption key?				D.5 Data Security Policy - Encryption	10.1.2	Key Management		3.6.1			
SL.32	Are clients provided with the ability to rotate their encryption key on a scheduled basis?				D.5 Data Security Policy - Encryption	10.1.2	Key Management		3.6.4			
SL.33	Are staff able to access client Scoped Data in an unencrypted state?				H.3 Logical Access Authorization	9.2.3 9.4.6	Management of privileged access rights Information access restriction		N/A			
SL.34	Are staff able to access client's encryption keys?				H.3 Logical Access Authorization	9.2.3 9.4.7	Management of privileged access rights Information access restriction		N/A			
SL.35	Is data segmentation and separation capability between clients provided?				V.1 Service and Deployment Models	9.4.1	Information access restriction		N/A			
SL.36	Does the ability exist to legally demonstrate sufficient data segmentation, in the event of a client subpoena or a forensics incident, so as not to impact other clients data if using resource pooling?				V.1 Service and Deployment Models	16.1.1 16.1.7	Responsibilities and Procedures, Collection of Evidence.		N/A			
SL.37	Is there a data classification retention program that identifies the data types that require additional management and governance?				P.1 Scoped Privacy Data Inventory and Flows	8.2	Information Classification		N/A			
SL.38	Is there a self-service portal or API call available to clients which provides the ability to place a "Legal hold" on client data which may be subject to a legal action, without impacting other clients data retention or destruction schedules?				P.6 Management of Client Scoped Privacy Data	16.1.1 16.1.7 18.1.2 18.1.3	Responsibilities and Procedures, Collection of Evidence, Intellectual Property Rights, Protection of records		N/A			
<b>E. Human Resource Security</b>												
SL.39	Is there a Human Resource policy approved by management, communicated to constituents and an owner to maintain and review? If yes, does it include:											ID-AM-6
SL.40	Security roles and responsibilities?				C.1 Security Organization Roles/Responsibilities	6.1.1	Information security roles and responsibilities		3.6.8 3.7		PO4.6, PO4.8, PO6.3, PO7.1, PO7.2, PO7.3, DS5.4	PR-AT-2 DE-DP-1
SL.41	Background screening?				E.2 Background Investigation Policy Content	7.1.1	Screening		12.7		N/A	
SL.42	Employment agreements?				E.3 Agreements for Constituents	7.1.2	Terms and conditions of employment		12.6.2		PO4.6, PO7.1, PO7.3, DS2.3	
SL.43	Security awareness training?				E.1 Security Awareness Training Program	7.2.2	Information security awareness, education, and training	Training and Culture: Training D1.TC.Tr.B.1 D1.TC.Tr.B.2	12.6	1.A.2	PO4.6, PO6.2, PO6.4, PO7.2, PO7.4, PO7.7, AI1.1, AI7.1, DS5.1, DSS.2, DS5.3, DS7.1, DS7.2	PR-AT-1
SL.44	Disciplinary process for non-compliance?				E.5 Separation Procedures	7.2.3	Disciplinary process	Training and Culture: Training D1.TC.C.B.1	N/A		PO4.8, PO7.8, DS5.6	
SL.45	Termination or change of status process?				E.5 Separation Procedures	7.3	Termination responsibilities	Preventative Controls: Access and Data Management D3.PC.ADM.B.5	N/A		PO4.8, PO7.8, DS5.6	
SL.46	Are background checks performed for Service Provider Contractors and Subcontractors?				E.2 Background Investigation Policy Content	7.1.1 7.2.1	Screening Management responsibilities		N/A	3.C.2		
SL.47	Do information security personnel have professional security certifications?					6.1.4	Contact with special interest groups			1.B.7(a)		
<b>F. Physical and Environmental Security</b>												
SL.48	Is there a physical security program?				F.2 Physical Security Controls - Scoped Data	5.1.1	Policies for information security		12.1		PO6.1, PO6.2, PO6.3, PO6.5, DS5.2, DS5.3, ME2.1	

Ques Num	SIG Question Text	Response	Maturity	Additional Information	AUP 2017 Relevance	ISO 27002:2013 Relevance	Appendix J Section and Line Reference	FFIEC CAT Tool_June 2015	PCI 3.2_April	FFIEC IT Mgmt	COBIT 4.1 Relevance	NIST Cybersecurity Framework_February2014
SL.49	Are physical security and environmental controls in the data center and office buildings?				F. Physical and Environmental Security	11.1 Secure areas		Preventative Controls: Access and Data Management Detective Controls: Event Detection D3.PC.ADM.B.11 D3.DC.ED.B.5	9.3		N/A	PR.AC-2 PR.IP-5 PR.MA-1 PR.PT-3 DE.CM-2
SL.50	Are visitors permitted in the facility?				F.7 Visitor Management	11.1.2 Physical entry controls		Preventative Controls: Access and Data Management Detective Controls: Event Detection D3.PC.ADM.B.11 D3.DC.ED.B.5	9.4		DS12.2, DS12.3	
<b>G. Operations Management</b>												
SL.51	Are management approved operating procedures utilized?				G. Operations Management	12.1.1 Documented Operating Procedure			11.6		A11.1, A14.4, DS13.1	
SL.52	Is there an operational change management/change control policy or program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?				G.1 Change Control	12.1.2 Change Management		Governance: IT Asset Management D1.G.IT.B.4	6.4	3.C.6	A16.1, A16.2, A16.3, A16.4, A16.5	
SL.53	Are backups of Scoped Systems and Data performed?				K.5 Backup Media Restoration	12.3.1 Information Back-Up		Incident Resilience Planning and Strategy: Testing D5.IR.PST.B.3	9.6.2		A16.1, A16.2, A16.3, A16.4, A16.5	PR.IP-4
SL.54	Are Cloud Services provided? If yes, what service model is provided (select all that apply):				V.1 Service and Deployment Models	4.3 Determining the scope of the information management system			N/A			
SL.55	Software as a Service (SaaS)?				V.1 Service and Deployment Models				N/A			
SL.56	Infrastructure as a Service (IaaS)?				V.1 Service and Deployment Models				N/A			
SL.57	Private cloud?				V.1 Service and Deployment Models				N/A			
SL.58	Public cloud?				V.1 Service and Deployment Models				N/A			
SL.59	Community cloud?				V.1 Service and Deployment Models				N/A			
SL.60	Hybrid cloud?				V.1 Service and Deployment Models				N/A			
SL.61	Is there a client management portal which allows distributed business accounts (business units/departments) to be managed under a single central corporate account?					15.2.1 Monitoring and review of supplier services			N/A			
SL.62	Are application self service features or an Internet accessible self-service portal available to clients?					9.4.1 Information access restriction			N/A			
SL.63	Can clients run their own security services within their own cloud environment?				V.3 Cloud Audit Program	12.4.1 12.4.3 12.5 12.6.1 Event logging, Administrator and operator logs, Control of operational software, Management of technical vulnerabilities			5.1, 5.2			
SL.64	Is there a management approved process to ensure that image snapshots containing Scoped Data are authorized prior to being snapped?					9.2.3 Management of privileged access rights			N/A			
SL.65	Is there a formal process to ensure clients are notified prior to changes being made which may impact their service? If yes, what is the communication method:				G.1 Change Control	12.1.2 Change management			6.4			
SL.66	Is there a scheduled maintenance window? If yes, what is the frequency:				V.4 Security Review of Hypervisor Configuration	12.6.1 Management of technical vulnerabilities			11.3.1, 11.3.2			
SL.67	Is there a scheduled maintenance window which results in client downtime? If yes, what is the downtime:				V.4 Security Review of Hypervisor Configuration	14.2.2.1 System change control procedures			N/A			
SL.68	Is there an online incident response status portal, which outlines planned and unplanned outages? If yes, how long after an unplanned outage is this updated:				J. Incident Event and Communications Management P.8 Privacy Incident Notification and Response Management	14.2.2 System change control procedures			N/A			PR.DS-5
<b>H. Access Control</b>												
SL.69	Are electronic systems used to transmit, process or store Scoped Systems and Data?								N/A		N/A	
SL.70	Are individual IDs required for user authentication to applications, operating systems, databases and network devices?				H.1 Password Controls	9.2.1.a User registration and de-registration		Preventative Controls: Access and Data Management D3.PC.ADM.B.6	8.1.1 12.3.2		DS5.4	PR.AC-1
SL.71	Are passwords used?				H. Access Control							
SL.72	Is there a password policy for systems that transmit, process or store Scoped Systems and Data that has been approved by management, communicated to constituents, and enforced on all platforms?				H. Access Control	9.4.3 Password Management System			8.1		DS5.3	
SL.73	Is remote access permitted?				H.8 Restrictions and Multifactor Authentication	6.2 Mobile devices and teleworking		Preventative Controls: Access and Data Management D3.PC.ADM.B.15	12.3.9		A11.2, A12.4, DS5.7, DS5.10, DS5.11	
SL.74	Is standards based federated ID capability available to clients (e.g., SAML, OpenID)?					9.2.1 User registration and de-registration			N/A			



Ques Num	SIG Question Text	Response	Maturity	Additional Information	AUP 2017 Relevance	ISO 27002:2013 Relevance	Appendix J Section and Line Reference	FFIEC CAT Tool_June 2015	PCI 3.2_April	FFIEC IT Mgmt	COBIT 4.1 Relevance	NIST Cybersecurity Framework_February2014
SL.75	Is two factor authentication required to access the production environment containing Scoped Data?					9.3.1	Use of secret authentication information		N/A			
SL.76	Are staff able to access client Scoped Data? If not, please identify the controls used to prevent this.				H.3 Logical Access Authorization	9.2.3 9.4.1	Management of privileged access rights Information access restriction		12.3.10			
SL.77	Is there a process which allows the client to specifically list who from the provider will have access to their Scoped Systems and Data?				H.3 Logical Access Authorization	9.1.1 9.2.3	Access Control Policy Management of privileged access rights		N/A			
<b>I. Application Security</b>												
SL.78	Are applications used to transmit, process or store Scoped Data?				I.1 Application Security Program Governance							
SL.79	Is a web site supported, hosted or maintained that has access to Scoped Systems and Data?								N/A		N/A	
SL.80	Are Web Servers used for transmitting, processing or storing Scoped Data? If yes, for all server platforms is/are:											
SL.81	Is HTTPS enabled for all web pages used as part of the scoped service?											
SL.82	All available high-risk security patches applied and verified at least monthly?											
SL.83	Are third party alert services used to keep up to date with the latest vulnerabilities?											
SL.84	Events relevant to supporting incident investigation regularly reviewed using a specific methodology to uncover potential incidents?							Monitoring and Analyzing: Monitoring and Analyzing	D2.MA.MA.B.2			
SL.85	Operating system and application logs relevant to supporting incident investigation protected against modification, deletion, and/or inappropriate access?											
SL.86	Is application development performed?				I. Application Security			Preventative Controls: Secure Coding Detective Controls: Threat and Vulnerability Detection	D3.PC.SC.B.3 D3.DC.TVD.B.1	N/A	A12.4, A17.4, A17.6, DS11.3, DS11.6	
SL.87	Is there a secure software development lifecycle policy (including mobile software applications) that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?				I.2 Secure Systems Development Lifecycle (SDLC) Policies, Standards and Procedures	14.2.1	Secure development policy		N/A	3.C.3 3.C.5		PR.IP-1 PR.IP-2 PR.IP-12
SL.88	Is development, test, and staging environment separate from the production environment? If so, how are they segmented:					12.1.4	Separation of development, testing and operational environments	Preventive Controls: Access and Data Management	D3.PC.ADM.B.10	6.4.1 6.4.3	N/A	PR.DS-7
SL.89	Is there a formal Software Development Life Cycle (SDLC) process?				I.2 Secure Systems Development Lifecycle (SDLC) Policies, Standards and Procedures	14.2.1	Secure development policy	Preventative Controls: Secure Coding	D3.PC.SC.B.1	6.3	A12.4, A17.4, A17.6, DS11.3, DS11.6	PR.IP-2 DE.CM-7
SL.90	Are change control procedures required for all changes to the production environment?				G.1 Change Control	9.4.5.g	Access control to program source code			6.4	A12.4, A17.4, A17.6, DS11.3, DS11.6	PR.IP-3
SL.91	Is Scoped Systems and Data ever used in the test, development, or QA environments? If yes, is:					14.3.1	Protection of test data			6.4.3	A13.3, DS2.4, DS9.1, DS9.2, DS11.6	
SL.92	Is there a documented change management / change control process? If yes, does it include:				G.1 Change Control	14.2.2	System change control procedures			6.4	A12.6, A16.2, A16.3, A17.2	
SL.93	Are compilers, editors or other development tools present in the production environment?				I.13 Production Application Vulnerability Monitoring Process	12.1.4.e	Separation of development, testing and operational environments			N/A	PO4.11, A13.4, A17.4	
SL.94	Is a secure code review performed at least annually?				I.2 Secure Systems Development Lifecycle (SDLC) Policies, Standards and Procedures	14.2.1	Secure development policy	Preventative Controls: Secure Coding	D3.PC.SC.B.2	6.3.2		
SL.95	Is each release subject to a full secure code review?				I.7 Secure Code Review	14.2.1	Secure development policy	Preventative Controls: Secure Coding	D3.PC.SC.B.2	N/A		
SL.96	Are applications analyzed on a regular basis to determine their vulnerability against recent attacks?				I.10 QA_UAT Process	12.2.1	Controls against malware			11.2.2		ID.RA-2 DE.CM-1
SL.97	Is there a formal development methodology in operation? If yes, which groups does it include?:				I.16 Secure Systems Development Lifecycle (SDLC) Reviews	12.5.1	Control of Operational Software			N/A		
SL.98	Are mobile applications that access Scoped Systems and Data developed?									N/A		
<b>J. Incident Event and Communications Management</b>												
SL.99	Is there an Incident Management Program that has been approved by management, communicated to constituents and an owner to maintain and review the program? If yes, does the program include:				J.1 Information Security / Information Technology Incident Management - Policy and Procedures Content	16	Information security incident management	Incident Resilience Planning and Strategy: Planning	D5.IR.PSP.B.1	11.1.2 12.10	3.C.3	N/A

Ques Num	SIG Question Text	Response	Maturity	Additional Information	AUP 2017 Relevance	ISO 27002:2013 Relevance	Appendix J Section and Line Reference	FFIEC CAT Tool_June 2015	PCI 3.2_April	FFIEC IT Mgmt	COBIT 4.1 Relevance	NIST Cybersecurity Framework_February2014
SL100	Privacy Incidents?				P.8 Privacy Incident Notification and Response Management	16.1 Management of information security incidents and improvements			N/A			
SL101	Is there a formal Incident Response Plan?				J. Incident Event and Communications Management	16.1.1.a.1 Responsibilities and procedures		Detection, Response, and Mitigation: Detection D5.DRM.D.B.3	12.10.1	3.C.3	PO9.3, DS5.6, DS8.2	PR.IP-9 RS.RP-1 RS.AN-2
SL102	Is there a 24x7x365 staffed phone number available to clients to report security incidents?				J. Information Security Incident Management P.8 Privacy Incident Notification and Response Management	15.1.1.h Information security policy for supplier relationships		Incident Resilience Planning and Strategy: Planning D5.IR.PSP.B.2	N/A			WP.1.E.3, WP.1.G.10
<b>K. Business Resiliency</b>												
SL103	Is there an established Business Resiliency program that has been approved by management and communicated to appropriate constituents?				K.1 Business Resiliency Governance	5.2 Management Commitment		Risk Management: Risk Management Program Incident Resilience Planning and Strategy: Planning D1.RM.RMP.B.1 D5.IR.PSP.B.6	N/A	1.B.4 3.C.4	N/A	ID.BE-5 PR.IP-9
SL104	Has a Business Impact Analysis been conducted?				K.2 Business Impact Analysis	8.2.2 Business impact analysis		Incident Resilience Planning and Strategy: Planning D5.IR.PSP.B.5	N/A	3.B	N/A	ID.BE-4 RS.AN-2
SL105	Is there a formal process focused on identifying and addressing risks of disruptive incidents to the organization?				K.3 Risk Assessment	8.2.3 Risk assessment			N/A	1.A.3 3.B	PO3.1, DS4.4, DS4.5, DS4.6, DS4.7, DS4.10	
SL106	Are specific response and recovery strategies defined for the prioritized activities?				K.4 Business Activity level Recovery Planning	8.3.1 Determination and selection			N/A	3.A.1	N/A	RS.IM-2
SL107	Are formal business continuity procedures developed and documented?				K.4 Business Activity level Recovery Planning	8.4 Establish and implement business continuity procedures			N/A		N/A	
SL108	Has senior management assigned the responsibility for the overall management of the response and recovery efforts?				K.1 Business Resiliency Governance				N/A		PO3.1, PO9.1, PO9.2, DS4.1, DS4.3, DS4.8, DS8.3	RS.CO-4 RC.CO-3
SL109	Is there a periodic (at least annual) review of your Business Resiliency Program?				K.6 Exercising	8.4.1 Establish and implement business continuity procedures						
SL110	Are there any dependencies on critical third party service providers?				K.2 Business Impact Analysis	8.1 8.3 8.3.1 8.44 Operational Planning and Control Business continuity strategy Determination and selection Business continuity plans	Strategic Considerations - Third Party Management. Line 124					
SL111	Is there a formal, documented exercise and testing program in place?				K.6 Exercising	8.5 Exercising and testing	Testing with Third Party TSPs lines 236-237					
SL112	Is there an Influenza Pandemic / Infectious Disease Outbreak Plan?				K.7 Infectious Disease Planning							
SL113	Is there a specific Recovery Time Objective (RTO)? If yes, what is it?					17.1.2 Implementing information security continuity			N/A			
SL114	Are all suppliers of critical hardware, network services and facility services involved in annual continuity and recovery tests?					17.1.3 Verify, review and evaluate information security continuity			N/A			
SL115	Are site failover tests performed at least annually?					17.1.3 Verify, review and evaluate information security continuity			N/A			
SL116	Do contracts with Critical Service Providers include a penalty or remediation clause for breach of availability and continuity SLAs?					15.1.2 15.2.1 Addressing security within supplier agreements, Monitoring and review of supplier services			N/A			
SL117	Is there sufficient redundancy capacity to ensure services are not impacted in multi-tenancy environments during peak usage and above?					17.1.3 Verify, review and evaluate information security continuity			N/A			
<b>L. Compliance</b>												
SL118	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?				L.3 Monitoring and Reporting - Compliance Requirement Identification	18.1.1 Identification of applicable legislation and contractual requirements			N/A	1.B.7 ( c ) 3.D.4	PO4.4, PO4.5, PO4.6, PO4.8, PO4.10, PO6.5, DS5.1, DSS.2, DS5.3	
SL119	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?				L.2 Monitoring and Reporting - Compliance				N/A		N/A	
SL120	Is there a records retention policy covering paper and electronic records, including email in support of applicable regulations, standards and contractual requirements?					18.1.3 Protection of records			N/A		PO4.8, DS11.2	
SL121	Is licensing maintained in all jurisdictions where required?								N/A		N/A	

Ques Num	SIG Question Text	Response	Maturity	Additional Information	AUP 2017 Relevance	ISO 27002:2013 Relevance	Appendix J Section and Line Reference	FFIEC CAT Tool_June 2015	PCI 3.2_April	FFIEC IT Mgmt	COBIT 4.1 Relevance	NIST Cybersecurity Framework_February2014
SL.122	Is there an documented internal compliance and ethics program to ensure professional ethics and business practices are implemented and maintained?				L.4 Professional Ethics and Business Practices				N/A		N/A	
SL.123	Are marketing or selling activities conducted directly to Client's customers?								N/A		N/A	
SL.124	Are there direct interactions with your client's customers?								N/A		N/A	
SL.125	Are documented policies and procedures maintained for enabling compliance with applicable legal, regulatory, or contractual obligations related to information security requirements?								N/A		N/A	ID.GV-3
SL.126	Is there a documented governance process to identify and assess changes that could significantly affect the system of internal controls for security, confidentiality and availability?				L.3 Monitoring and Reporting - Compliance Requirement Identification				N/A		N/A	
SL.127	Are accounts opened, transactions initiated or other account initiation activity applying payments, taking payments, transferring funds, etc. through either electronic, telephonic, written or in-person requests made on behalf of your client's?											
SL.128	Are these sites, applications and systems used to also transmit, process or store non-scoped data?											
SL.129	Are all transaction details (such as payment card info and information about the parties conducting transactions) prohibited from being stored in the DMZ?					14.1.3.e	Protecting Application Services Transactions		N/A			
SL.130	Does the service provider permit client audits and assessments?				V.3 Cloud Audit Program	15.1.2 15.2.1	Addressing security within supplier agreements, Monitoring and review of supplier services		10.8			
<b>M. End User Device Security</b>												
SL.131	Are End User Devices (Desktops, Laptops, Tablets, Smartphones) used for transmitting, processing or storing Scoped Data? If yes, for all platforms, are:											
SL.132	Security configuration standards documented? If yes, are:											
SL.133	All available high-risk security patches applied and verified at least monthly on all server platforms?											
SL.134	Sufficient detail contained in Operating System and application logs to support incident investigation, including successful and failed login attempts and changes to sensitive configuration settings and files?											
SL.135	Operating system and application logs relevant to supporting incident investigation protected against modification, deletion, and/or inappropriate access?											
SL.136	Are constituents allowed to utilize mobile devices within your environment? If yes, which of the following functions are allowed:								N/A			
SL.137	View Scoped Data?								N/A			

# 2017 SHARED ASSESSMENTS SIG LITE OVERVIEW

## ABOUT THE SIG LITE

The Standardized Information Gathering (SIG) questionnaire is a holistic tool for risk management assessments, including assessments of cybersecurity, IT, privacy, data security and business resiliency controls. The SIG Lite is generally used for third party service providers who offer lower risk services, but can also be used as a starting point to conduct an initial assessment of all service providers. Because it is a compilation of all of the high level questions from the detail tabs of the full SIG, the SIG Lite allows a user to get an initial assessment of the service provider’s risk controls. Users have the ability to follow up with the full SIG if additional details about risk controls are required. The Standardized Information Gathering (SIG) questionnaire is developed using high level questions followed by additional detailed sub-questions. This allows the user of the SIG to obtain detailed information about certain risk control areas. However, there are many occasions where a “high level” assessment of a particular risk control area is sufficient.

SIG Lite					
0% Percent Complete					Tab Automation:
<b>Questionnaire Instructions:</b>					
- 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 and disable the transfer of responses from the Lite 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.					
Ques Num	Question/Request	Response	Maturity	Additional Information	AUP Reference
<b>A. Risk Assessment and Treatment</b>					
SL.1	Is there a risk assessment program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the program?				A.1 IT & Infrastructure Risk Governance and Context
<b>B. Security Policy</b>					
SL.2	Is there an information security policy that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?				B.1 Information Security Policy Content & Maintenance
SL.3	Have the policies been reviewed in the last 12 months?				B.1 Procedure: d
SL.4	Is there a vendor management program?				
<b>C. Organizational Security</b>					
SL.5	Is there a respondent information security function responsible for security initiatives?				C.2 Security Organization Roles / Responsibilities
SL.6	Do external parties have access to Scoped Systems and Data or processing				

## HOW TO USE THE SIG LITE

This section describes how to use the SIG Lite as a standalone document.

### Creating a Master SIG Lite

The creation of a Master SIG Lite allows the issuer to compare the SIG Lite received from a provider to the set of high level risk controls it believes should be in place. This facilitates the identification of risk control areas that require additional examination, and/or areas that require remediation. It is useful for a company that issues the SIG Lite to a third party provider (the “assessee”) to create a Master SIG Lite for each provider type.

## SIG Lite Management Tool (SMT)

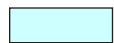
The SMT is a companion tool to the SIG Lite and performs two primary functions:

1. Automates the ability to compare a Master SIG Lite to SIG Lites received from assesseees by producing a detailed report that identifies discrepancies between the desired responses in the master SIG Lite and the responses returned by the provider.
2. Allows a user to transfer responses between SIG Lite versions, facilitating transfer of responses to a newer version of the SIG Lite and leaving blank only questions not previously addressed. It also facilitates the transfer between versions of the SIG Lite, should that be required. *This is particularly important as the SMT Lite can only compare SIG Lites of equal version.*

## SIG & SIG LITE Color Key

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

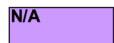
**The following are the colors used in the SIG and a description for each:**



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



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



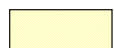
**PURPLE BACKGROUND IN A CELL** identifies a “N/A” response to a question, whether or not the word “N/A” appears. If the letters “N/A” do not appear in a purple cell, then the response was inherited by the answer to its top-level question (see “Question Hierarchy” section for more detail).



**ORANGE BACKGROUND IN A CELL** identifies a “No” response to a question, whether or not the word “No” appears. If the word “No” does not appear in an orange cell, then the response was inherited by the answer to its top-level question (see “Question Hierarchy” section for more detail).



**CELLS WITH A HASH BACKGROUND** are not to be filled in; rather they are a primary question that has sub-questions (secondary questions) below.



**A YELLOW BACKGROUND IN SECTION HEADER AT THE TOP OF A TAB** indicates the tab is incomplete. In addition to being found in an incomplete tab, the yellow background will appear on the Dashboard, Lite and Business Information tabs to indicate where responses are still required.



**A GREEN BACKGROUND IN SECTION HEADER AT THE TOP OF A TAB** indicates the tab is complete. In addition to being found in a complete tab, the green background will appear on the Dashboard, Lite and Business Information tabs to indicate where responses are still required.

## **Question Hierarchy**

SIG questions are arranged hierarchically, meaning that top-level questions are followed by sub-questions when appropriate. This hierarchy is identified by the question number and the number of digits and separators (a period), which identify the relationship of the question (e.g., question A.1.1 is a sub-level of A.1). If a “No” or “N/A” response is provided for question A.1, question A.1.1 will inherit that response. This inheritance is indicated by the background color of the response cell (see SIG Color Key above).

## **Maturity Field**

For a robust review, Maturity and Binary should go hand-in-hand. The Maturity value will help to provide an additional dimension to the question response. The assessee would identify if a control is in place and, if it is, then they can identify the level of maturity for that question. The Maturity field is used by the assessee to identify how mature the question is within the environment. In some cases a “Yes” or “No” response may not provide the full picture of the control environment under review.

The levels of Maturity are from Level 1 through Level 5, with 1 being the lowest Maturity and 5 being the highest level to be achieved. The levels are defined as follows:

- Level 1: Informal, ad hoc process without formal implementation.
- Level 2: Partially in place with no approved plans to further implement.
- Level 3: Partially in place with approved plans to further implement.
- Level 4: In place with exclusions.
- Level 5: In place with no exclusions.

## **SIG Lite Errors and Recovery**

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

## **LEARN MORE**

To learn more, purchase the Shared Assessments Program Tools or to obtain information about membership opportunities, contact us at [info@sharedassessments.org](mailto:info@sharedassessments.org).