SIG Lite

100% 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	
A. Risk Assessment and Treatment							
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:	Yes	4		A.1 IT & Infrastructure Risk Governance and Context	5.1 6.1.2	Leadership & Commitment, Information Security Risk Assessment
SL.2	Is there a program to manage the treatment of risks identified during assessments?	Yes	5		A.2 IT & Infrastructure Risk Assessment Life Cycle	6.1.3	Information Security Risk treatment
SL.3	A formal process for assigning appropriate management ownership for each risk?	Yes	5		A.2 IT & Infrastructure Risk Assessment Life Cycle		
SL.4	A formal process for appropriate management knowingly and objectively accepting risks and approving action plans?	Yes	5		A.2 IT & Infrastructure Risk Assessment Life Cycle		
SL.5	A formal process for tracking the status of action plans and reporting them to management?	Yes	5		A.2 IT & Infrastructure Risk Assessment Life Cycle		
SL.6	Controls identified for each material risk?	Yes	4		A.2 IT & Infrastructure Risk Assessment Life Cycle		
SL.7	Measures for defining, monitoring, and reporting risk metrics?	Yes	5		A.2 IT & Infrastructure Risk Assessment Life Cycle		
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:	Yes	4			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:	Yes	5		A.7 Subcontractor Selection and Management Process	15.1.1	Information security policy for supplier relationships
SL.10	Approval by management?	Yes	5		A.7 Subcontractor Selection and Management Process	5.1.1	Policies on information security
SL.11	Annual review?	Yes	5		A.7 Subcontractor Selection and Management Process	5.1.2	Review of the policies for information security
SL.12	Required reassessment when service delivery or contract changes?	Yes	5				
SL.13	Review of the subcontractor's vendor management policy and procedures?	Yes	3		A.9 Documenting Information Security Assessments for Subcontractors	15.2.1.g	Monitoring and review of supplier services
SL.14	Is there a process to identify and log subcontractor information security, privacy and/or data breach issues?	Yes	5		A.9 Documenting Information Security Assessments for Subcontractors	15.2.1.e	Monitoring and review of supplier services
SL.15	Is there a vendor management program?	Yes	5		A.5 Vendor Risk Management Program		
SL.16	Do external parties have access to Scoped Systems and Data or processing facilities?	No				15	Supplier relationships

Ques Num	Question/Request	Response	Maturity	Additional Information	AUP Reference	ISO 27002:2013 Relevance	
SL.17	Is the maturity of IT management processes formally evaluated at least annually using an established benchmark (e.g., COBIT maturity models)?	Yes	1			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.	Yes	5	Privacy risk assessments are completed when planning new features, services, when there are material changes, regulatory changes, or part of the annual review.	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?	Yes	5		P.3 Privacy Organization and Program Maintenance	15.1.1.l	Information security policy for supplier relationships
SL.20	Are reasonable resources (in time and money) allocated to mitigating identified privacy risks?	Yes	5		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?	N/A			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?	Yes	3		P.3 Privacy Organization and Program Maintenance		
B. Security Policy							
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?	Yes	4	The information security policies are owned by the VP of Hosted Operations	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?	Yes			B.1 Information Security Policy Maintenance	5.1.2	Review of the policies for information security
C. Organizational Security							
SL.25	Is there a respondent information security function responsible for security initiatives?	Yes	4		C.1 Security Organization Roles / Responsibilities	6.1.1	Information Security Roles and Responsibilities
D. Asset and Information Management							
SL.26	Is there an asset management policy approved by management, communicated to constituents and an owner to maintain and review?	Yes	4		D. Asset and Information Management	8.1	Responsibility for Assets
SL.27	Is information classified?	Yes	5		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?	Yes	5		D.4 Removable Device Security	8.3.1	Management of Removable Media
SL.29	Is Scoped Data sent or received via physical media?	No			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:	Yes	5		D.5 Data Security Policy - Encryption	10.1	Cryptographic controls
SL.31	Are clients provided with the ability to generate a unique encryption key?	No			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?	No			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?	Yes	4		H.3 Logical Access Authorization	9.2.3 9.4.6	Management of privileged access rights Information access restriction
SL.34	Are staff able to access client's encryption keys?	Yes	5		H.3 Logical Access Authorization	9.2.3 9.4.7	Management of privileged access rights Information access restriction

Ques Num	Question/Request	Response	Maturity	Additional Information	AUP Reference	ISO 27002:2013 Relevance	
SL.35	Is data segmentation and separation capability between clients provided?	Yes	5		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?	Yes	5		V.1 Service and Deployment Models	16.1.1 16.1.7	Responsibilities and Procedures, Collection of Evidence.
SL.37	Is there a data classification retention program that identifies the data types that require additional management and governance?	Yes	5		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?	Yes	5	Client would make a legal hold request using our support portal.	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
E. Human Resource Security							
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:	Yes	4				
SL.40	Security roles and responsibilities?	Yes	4		C.1 Security Organization Roles/Responsibilities	6.1.1	Information security roles and responsibilities
SL.41	Background screening?	Yes	4		E.2 Background Investigation Policy Content	7.1.1	Screening
SL.42	Employment agreements?	Yes	4		E.3 Agreements for Constituents	7.1.2	Terms and conditions of employment
SL.43	Security awareness training?	Yes	4		E.1 Security Awareness Training Program	7.2.2	Information security awareness, education, and training
SL.44	Disciplinary process for non-compliance?	Yes	4		E.5 Separation Procedures	7.2.3	Disciplinary process
SL.45	Termination or change of status process?	Yes	4		E.5 Separation Procedures	7.3	Termination responsibilities
SL.46	Are background checks performed for Service Provider Contractors and Subcontractors?	Yes	4		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?	Yes	4			6.1.4	Contact with special interest groups
F. Physical and Environmental Security							
SL.48	Is there a physical security program?	Yes	4		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?	Yes	4	The data center is provided by Rackspace which maintains the physical security and environmental controls.	F. Physical and Environmental Security	11.1	Secure areas
SL.50	Are visitors permitted in the facility?	Yes	4	Customers of Rackspace are permitted to visit their facilities.	F.7 Visitor Management	11.1.2	Physical entry controls
G. Operations Management							
SL.51	Are management approved operating procedures utilized?	Yes	4		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?	Yes	4		G.1 Change Control	12.1.2	Change Management

Ques Num	Question/Request	Response	Maturity	Additional Information	AUP Reference	ISO 27002:2013 Relevance	
SL.53	Are backups of Scoped Systems and Data performed?	Yes	4		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):	Yes	5		V.1 Service and Deployment Models	4.3	Determining the scope of the information management system
SL.55	Software as a Service (SaaS)?	Yes	5		V.1 Service and Deployment Models		
SL.56	Infrastructure as a Service (IaaS)?	No			V.1 Service and Deployment Models		
SL.57	Private cloud?	Yes	5		V.1 Service and Deployment Models		
SL.58	Public cloud?	No			V.1 Service and Deployment Models		
SL.59	Community cloud?	No			V.1 Service and Deployment Models		
SL.60	Hybrid cloud?	No			V.1 Service and Deployment Models		
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?	Yes	5			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?	Yes	4			9.4.1	Information access restriction
SL.63	Can clients run their own security services within their own cloud environment?	No			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
SL.64	Is there a management approved process to ensure that image snapshots containing Scoped Data are authorized prior to being snapped?	Yes	5			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:	Yes	5	Email to the primary client adminstrator, notifications on the Spigit customer hub.	G.1 Change Control	12.1.2	Change management
SL.66	Is there a scheduled maintenance window? If yes, what is the frequency:	Yes	5	Every Friday at midnight server time.	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:	Yes	5	Down time does not occur at every maintenance window, but if it should occur, downtime would be less than 5 minutes	V.4 Security Review of Hypervisor Configuration	14.2.2.l	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:	Yes	5	This Spigit Support portal is updated within 24 hours	J. Incident Event and Communications Management P.8 Privacy Incident Notification and Response Management	14.2.2	System change control procedures
H. Access Control							
SL.69	Are electronic systems used to transmit, process or store Scoped Systems and Data?	Yes	5				

Ques Num	Question/Request	Response	Maturity	Additional Information	AUP Reference	ISO 27002:2013 Relevance	
SL.70	Are individual IDs required for user authentication to applications, operating systems, databases and network devices?	Yes	5		H.1 Password Controls	9.2.1.a	User registration and de-registration
SL.71	Are passwords used?	Yes	5		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?	Yes	5		H. Access Control	9.4.3	Password Management System
SL.73	Is remote access permitted?	Yes	5		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)?	Yes	5			9.2.1	User registration and de-registration
SL.75	Is two factor authentication required to access the production environment containing Scoped Data?	Yes	5	All Spigit staff require two factor authentication to access client 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.	Yes	5	Support staff are able to access.	H.3 Logical Access Authorization	9.2.3 9.4.1	Management of privileged access rights 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?	Yes	5		H.3 Logical Access Authorization	9.1.1 9.2.3	Access Control Policy Management of privileged access rights
I. Application Security							
SL.78	Are applications used to transmit, process or store Scoped Data?	Yes	5		I.1 Application Security Program Governance		
SL.79	Is a web site supported, hosted or maintained that has access to Scoped Systems and Data?	Yes	5				
SL.80	Are Web Servers used for transmitting, processing or storing Scoped Data? If yes, for all server platforms is/are:	Yes	5	Apache running on CentOS			
SL.81	Is HTTPS enabled for all web pages used as part of the scoped service?	Yes	5				
SL.82	All available high-risk security patches applied and verified at least monthly?	Yes	5				
SL.83	Are third party alert services used to keep up to date with the latest vulnerabilities?	Yes	5				
SL.84	Events relevant to supporting incident investigation regularly reviewed using a specific methodology to uncover potential incidents?	Yes	4				
SL.85	Operating system and application logs relevant to supporting incident investigation protected against modification, deletion, and/or inappropriate access?	Yes	5				
SL.86	Is application development performed?	Yes	5		I. Application Security		
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?	Yes	4		I.2 Secure Systems Development Lifecycle (SDLC) Policies, Standards and Procedures	14.2.1	Secure development policy
SL.88	Is development, test, and staging environment separate from the production environment? If so, how are they segmented:	Yes	5	Separate and unique application stacks are used. In addition, production and staging sites are located on different physical servers		12.1.4	Separation of development, testing and operational environments

Ques Num	Question/Request	Response	Maturity	Additional Information	AUP Reference	ISO 27002:2013 Relevance	
SL.89	Is there a formal Software Development Life Cycle (SDLC) process?	Yes	5		I.2 Secure Systems Development Lifecycle (SDLC) Policies, Standards and Procedures	14.2.1	Secure development policy
SL.90	Are change control procedures required for all changes to the production environment?	Yes	5		G.1 Change Control	9.4.5.g	Access control to program source code
SL.91	Is Scoped Systems and Data ever used in the test, development, or QA environments? If yes, is:	No				14.3.1	Protection of test data
SL.92	Is there a documented change management / change control process? If yes, does it include:	N/A			G.1 Change Control	14.2.2	System change control procedures
SL.93	Are compilers, editors or other development tools present in the production environment?	No			I.13 Production Application Vulnerability Monitoring Process	12.1.4.e	Separation of development, testing and operational environments
SL.94	Is a secure code review performed at least annually?	No			I.2 Secure Systems Development Lifecycle (SDLC) Policies, Standards and Procedures	14.2.1	Secure development policy
SL.95	Is each release subject to a full secure code review?	No		Only changed or added code goes through review	I.7 Secure Code Review	14.2.1	Secure development policy
SL.96	Are applications analyzed on a regular basis to determine their vulnerability against recent attacks?	Yes	4		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?:	Yes	4	Engineering and operations	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?	No					
J. Incident Event and Communications Management							
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:	Yes	3		J.1 Information Security / Information Technology Incident Management - Policy and Procedures Content	16	Information security incident management
SL.100	Privacy Incidents?	Yes	5		P.8 Privacy Incident Notification and Response Management	16.1	Management of information security incidents and improvements
SL.101	Is there a formal Incident Response Plan?	Yes	5		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?	Yes	5		J. Information Security Incident Management P.8 Privacy Incident Notification and Response Management	15.1.1.h	Information security policy for supplier relationships
K. Business Resiliency							
SL.103	Is there an established Business Resiliency program that has been approved by management and communicated to appropriate constituents?	Yes	3		K.1 Business Resiliency Governance	5.2	Management Commitment

Ques Num	Question/Request	Response	Maturity	Additional Information	AUP Reference	ISO 27002:2013 Relevance	
SL.104	Has a Business Impact Analysis been conducted?	Yes	3		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?	Yes	3		K.3 Risk Assessment	8.2.3	Risk assessment
SL.106	Are specific response and recovery strategies defined for the prioritized activities?	Yes	4		K.4 Business Activity level Recovery Planning	8.3.1	Determination and selection
SL.107	Are formal business continuity procedures developed and documented?	Yes	3		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?	Yes	4		K.1 Business Resiliency Governance		
SL.109	Is there a periodic (at least annual) review of your Business Resiliency Program?	Yes	3		K.6 Exercising	8.4.1	Establish and implement business continuity procedures
SL.110	Are there any dependencies on critical third party service providers?	Yes	4	Spigit relies on RackSpace as its hosting provider and GoodData for Analytics	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
SL.111	Is there a formal, documented exercise and testing program in place?	Yes	3		K.6 Exercising	8.5	Exercising and testing
SL.112	Is there an Influenza Pandemic / Infectious Disease Outbreak Plan?	Yes	4		K.7 Infectious Disease Planning		
SL.113	Is there a specific Recovery Time Objective (RTO)? If yes, what is it?	Yes	5	4 hours		17.1.2	Implementing information security continuity
SL.114	Are all suppliers of critical hardware, network services and facility services involved in annual continuity and recovery tests?	Yes	5			17.1.3	Verify, review and evaluate information security continuity
SL.115	Are site failover tests performed at least annually?	Yes	4			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?	Yes				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?	Yes				17.1.3	Verify, review and evaluate information security continuity
L. Compliance							
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?	Yes	4		L.3 Monitoring and Reporting - Compliance Requirement Identification	18.1.1	Identification of applicable legislation and contractual requirements

Ques Num	Question/Request	Response	Maturity	Additional Information	AUP Reference	ISO 27002:2013 Relevance	
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?	Yes	4		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?	Yes	4			18.1.3	Protection of records
SL.121	Is licensing maintained in all jurisdictions where required?	Yes	4				
SL.122	Is there an documented internal compliance and ethics program to ensure professional ethics and business practices are implemented and maintained?	Yes	4		L.4 Professional Ethics and Business Practices		
SL.123	Are marketing or selling activities conducted directly to Client's customers?	No					
SL.124	Are there direct interactions with your client's customers?	No					
SL.125	Are documented policies and procedures maintained for enabling compliance with applicable legal, regulatory, or contractual obligations related to information security requirements?	Yes	4				
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?	Yes	4		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?	N/A		Spigit does not store or process financial transactions.			
SL.128	Are these sites, applications and systems used to also transmit, process or store non-scoped data?	N/A					
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?	N/A		Spigit does not store or process financial transactions.		14.1.3.e	Protecting Application Services Transactions
SL.130	Does the service provider permit client audits and assessments?	Yes	5		V.3 Cloud Audit Program	15.1.2 15.2.1	Addressing security within supplier agreements, Monitoring and review of supplier services
M. End User Device Security							
SL.131	Are End User Devices (Desktops, Laptops, Tablets, Smartphones) used for transmitting, processing or storing Scoped Data? If yes, for all platforms, are:	No					
SL.136	Are constituents allowed to utilize mobile devices within your environment? If yes, which of the following functions are allowed:	Yes	4				
SL.137	View Scoped Data?	No					
SL.138	Process Scoped Data?	No					
SL.139	Delete Scoped Data?	No					
SL.140	Store Scoped Data?	No					
SL.141	Is there a mobile device management program in place that has been approved by management and communicated to appropriate constituents?	Yes	3				
SL.142	Is there a Mobile Device Management solution in place?	Yes	5				

Ques Num	Question/Request	Response	Maturity	Additional Information	AUP Reference	ISO 27002:2013 Relevance	
SL.143	Is there an approved process for IT to off-board mobile devices when a constituent terminates, or requests to on-board a new mobile device? If yes, does it:	Yes	5				
SL.144	Are staff technically prevented from accessing the administrative environment via non-managed private devices? If yes, is it from:	No			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
N. Network Security							
SL.145	Are there external network connections (Internet, extranet, etc.)?	Yes	5		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)?	Yes	5		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?	Yes			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?	Yes	5			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?	Yes	5			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?	Yes	5		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?	No			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?	Yes			H.3 Logical Access Authorization	12.4.1 15.2.1	Event Logging, Monitoring and review of supplier services
P. Privacy							
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.	Yes	4	username, first name, last name, and company email address..		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?	Yes	5		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?	No		No PKI is processed by Spigit	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.	Yes	5	Clients determine who has access to the Spigit application and if the allow access from outside the US.			

Ques Num	Question/Request	Response	Maturity	Additional Information	AUP Reference	ISO 27002:2013 Relevance	
SL.157	Is personal information transmitted, processed, stored, or disclosed to or retained by third parties? If yes, describe.	Yes	5	Sub processors are provided data under data processing agreements that include security and privacy requirements		15	Supplier Relationships
SL.158	Are there contractual controls to ensure that personal information transmitted, processed, stored or disclosed to or retained by third parties is limited to defined parameters for access, use and disclosure? If yes, describe. If no, explain reason.	Yes	5		P.4 Third Party Privacy Agreements	15.1.2	Addressing security within supplier agreements
SL.159	Is personal information accessed, disclosed, processed, transmitted or retained with third parties outside the US? If yes, describe and list the countries.	Yes	5	A limited group of users are allowed to use our learning management system which is hosted in Canada.		15	Supplier Relationships
SL.160	Is there a documented privacy policy or procedures for the protection of information transmitted, processed, or maintained on behalf of the client?	Yes	5		P.2 Privacy Policy and Privacy Notices	15.1.1	Information security policy for supplier relationships
SL.161	Are transactions for covered accounts accessed, modified, or processed, including address changes and discrepancies? If yes, describe.	N/A		No account processing occurs.			
T. Threat Management							
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?	Yes	5		T.1 Virus Protection (Servers) T.2 Virus Protection (Workstations)	12.2.1	Controls Against Malware
SL.163	Prohibition of disabling anti-malware with exceptions requiring Security approval and reenablement as soon as possible.	Yes	5				
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?	Yes	5		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?	Yes	5		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?	Yes	5				
SL.167	Are penetration tests performed?	Yes	5				
SL.168	Are there processes to manage threat and vulnerability assessment tools and the data they collect?	Yes	5		I.1 Application Security Program Governance	12.6.1	Management of technical vulnerabilities
U. Server Security							
SL.169	Are Servers used for transmitting, processing or storing Scoped Data?	Yes	5				
SL.170	Are systems and applications patched?	Yes	5		G.2 System Patching	12.6.1	Management of technical vulnerabilities
SL.171	Are default hardened base virtual images applied to virtualized operating systems?	N/A		virtualization is not used	U.2 System Hardening Standards		
SL.172	Are Hypervisors used to manage systems used to transmit, process or store Scoped Data?	No			V.4 Security Review of Hypervisor Configuration	14.1.2	Securing application services on public networks