CSA CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE (CAIQ) – LITE V3.0.1

JUNE 2020

Social Solutions

NOTICE

This information is provided for evaluation purposes only, so your organization may review SSG's security processes and controls to determine whether the products and services meet your needs. This questionnaire is not made part of any agreement you may sign with SSG, and does not constitute a representation or warranty on the part of SSG.

TABLE OF CONTENTS

ABSTRACT

The Cloud Security Alliance is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. The Cloud Security Alliance ("CSA") is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholders. In order to accommodate the shift to cloud procurement models, CSA and Whistic identified the need for a streamlined assessment questionnaire to better arm cybersecurity professionals to efficiently engage their cloud vendors.

The CAIQ offers an industry-accepted way to document what security controls exist in IaaS, PaaS, and SaaS services, providing security control transparency. It provides a set of Yes/No questions a cloud consumer and cloud auditor may wish to ask of a cloud provider to ascertain their compliance to the Cloud Controls Matrix (CCM). Therefore, it helps cloud customers to gauge the security posture of prospective cloud service providers and determine if their cloud services are suitably ("CSA") secure.

CAIQ-Lite was developed to match the rapid pace inherent within the cybersecurity environment, placing increased importance on vendor security questionnaire adoption.

For more information, see https://cloudsecurityalliance.org.

CSA CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE – LITE

The questionnaire has been completed using the current CSA CAIQ-Lite standard, v3.0.1

QUESTION ID	CONSENSUS ASSESSMENT QUESTIONS	CONSENSUS ASSESSMENT ANSWERS			NOTES
		YES	NO	N/A	
AIS-01.2	Do you use an automated source code analysis tool to detect security defects in code prior to production?		X		As a compensating control, dynamic application security scans are conducted against live versions of the application at least quarterly.
AIS-01.5	(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	X			Each code change is required to be approved by two peers of the code's author before deployment to a staging environment. Testing is conducted and issues are addressed, before deployment to production environments.
AIS-02.1	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems?	X			All identified requirements are addressed contractually before customers can access the full application. Any remediation efforts take place before the customer is granted access.
AIS-03.1	Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	X			Controls in place to prevent systematic errors and the corruption of data include application error handling, audit trails, SQL replication, and daily backups. Controls in place to prevent most manual errors and corruption of data include application access controls and input validation.
AAC-02.1	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	X			SSG provides third-party attestations and SOC2 Type II reports directly to our customers under NDA.
AAC-02.2	Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?	X			External vulnerability threat assessments are performed regularly by independent security firms.

AAC-02.3	Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	X			Application penetration tests are conducted on an annual cadence by a third-party security firm under contract by SSG. Identified vulnerabilities are remediated and re-tested by the third-party security firm.
AAC-03.1	Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	X			Customer data is segregated from all other customer data via logical controls built into the application, databases, and infrastructure preventing any access, intentional or inadvertent, to another customer's data.
AAC-03.2	Do you have the capability to recover data for a specific customer in the case of a failure or data loss?	X			Backups are taken nightly and retained for 13 months for each individual customer database, allowing for the capability to restore a specific customer's data in the event of failure or data loss.
BCR-02.1	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	X			The business continuity and disaster recovery plans are reviewed annually, and the disaster recovery plan is tested annually.
BCR-09.1	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	X			Active customers have access to a live dashboard that shows the current and historical uptime for ETO services.
BCR-10.1	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	X			Policies regarding the governance, operation, and support of IT/Cloud Operations including the information security policy, technical change management policy, acceptable use policy, etc., are made available to all employees.
BCR-11.1	Do you have technical control capabilities to enforce tenant data retention policies?	X			Technical controls enforcing data retention policies include replication across AWS availability zones, nightly backups to private encrypted AWS S3 buckets, and a disaster recovery hot site in a separate AWS region.
BCR-11.4	Have you implemented backup or redundancy mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	X			SQL backups are automatically performed nightly, replicated across multiple AWS regions for disaster recovery purposes.

BCR-11.5	Do you test your backup or redundancy mechanisms at least annually?	X			Backup and redundancy mechanisms are monitored in real time and for job completion in the case of nightly jobs. Errors are alerted upon and remediated according to an escalation policy. The backups are tested monthly at a minimum.
CCC-01.2	Is documentation available that describes the installation, configuration, and use of products/services/features?	X			Training documentation, videos, and support blogs are available to customers for the configuration and use of the application and its features.
CCC-04.1	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	X			SSG's acceptable use policy includes the principal of least privilege, only employees with a documented business need are granted administrative access to their company-owned endpoints. All company-owned employee endpoints are monitored via asset management software that audits software installations.
DSI-03.1	Do you provide open encryption methodologies (3.4ES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?	X			All traffic to and from the application is encrypted via the TLS protocol, an open encryption standard.
DSI-03.2	Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?	X			Communications over public networks, between our infrastructure components, is encrypted via the TLS protocol, an open encryption standard.
DSI-05.1	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	X			Access to production systems and data is restricted to only those of the Cloud Operations team. Unless authorized contractually, or by explicit written consent, no customer data resides outside of the production systems without a de-identification of the data subject to the terms of customer's agreement.

DSI-07.1	Do you support secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data as determined by the tenant?	X			Client data backups are taken nightly and retained for 13 months for each individual customer database. Each tenant's archived and backed-up database will be deleted 13 months after termination via an automated data lifecycle. This control is partially inherited from our cloud hosting provider. For updated information on the control language, please see the policies linked here.
DSI-07.2	Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	X			Terms for exiting the service agreement are defined in the customer's MSA. Refer to DSI-07.1 for assurance to sanitize once SSG is no longer the data custodian.
DCS-01.1	Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset?	X			All assets are tracked and owned by the Cloud Operations team. Each asset is monitored by cloud tools and third-party infrastructure monitoring platforms to ensure complete asset tracking capabilities across the application infrastructure.
DCS-02.1	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented?	X			This control is inherited from our cloud hosting provider. For updated information on the control language, please see the policies linked here.
DCS-09.1	Do you restrict physical access to information assets and functions by users and support personnel?	X			This control is inherited from our cloud hosting provider. For updated information on the control language, please see the policies linked here.
EKM-02.1	Do you have a capability to allow creation of unique encryption keys per tenant?		X		SSG does not support unique keys per customer.
EKM-03.1	Do you encrypt tenant data at rest (on disk/storage) within your environment?	X			Any location that customer data is stored is encrypted using AES 256-bit encryption at a minimum. This includes, but is not limited to, SQL data drives, private AWS S3 buckets, and backup locations.

GRM-01.1	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?	X			New infrastructure is built with predefined AWS AMIs that include a default security baseline. All non-AWS managed infrastructure is scanned weekly for vulnerabilities and remediated according to NIST 800-53 remediation timelines. For all AWS managed systems, AWS is in alignment with ISO 27001 standards, and maintains system baselines for critical components. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
GRM-06.1	Do your information security and privacy policies align with industry standards (ISO-27001, ISO-22307, CoBIT, etc.)?	X			SSG's information security and privacy policies align with SSAE-18.
GRM-07.1	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	X			A formal disciplinary policy is included in SSG's employee handbook and information security policy that includes sanctions up to and including termination.
GRM-09.1	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	X			Any material changes to customer facing information security and privacy policies are made available to active customers and prospective customers under NDA and/or confidentiality provisions in existing agreements.
GRM-09.2	Do you perform, at minimum, annual reviews to your privacy and security policies?	X			The SSG Information Security and Legal teams review the information security and privacy policies on at least an annual cadence.
HRS-01.1	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?	X			Production systems are monitored by AWS CloudWatch and Guard Duty. Notifications of potentially unauthorized access are alerted upon and investigated with AWS provided logs. Once a privacy event would be confirmed, impacted customers will be notified without due delay.
HRS-02.1	Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification?	X			All SSG employees and contractors undergo a background verification as a condition of employment.

HRS-03.1	Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	X			All SSG new hires are required to successfully complete information security, privacy, and HIPAA training. All SSG employees are required to complete this training annually.
HRS-03.3	Are all personnel required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information?	X			All SSG employees and contractors sign an NDA as a condition of employment that covers the protection of customer information.
HRS-03.5	Are personnel trained and provided with awareness programs at least once a year?	X			All SSG employees are required to complete information security, privacy, and HIPAA training annually.
HRS-04.1	Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination?	X			The SSG employee handbook and information security policies govern changes in employment including termination.
IAM-01.1	Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)?	X			Security management systems that impact production applications are restricted to authorized personnel. All access is logged and audited for compliance. AWS managed systems are in alignment with ISO 27001 standards, AWS has established formal policies, procedures to delineate the minimum standards for logical access to AWS resources.
IAM-01.2	Do you monitor and log privileged access (e.g., administrator level) to information security management systems?	X			Security management systems that impact production applications are restricted to authorized personnel. All privileged access is logged and audited for compliance. AWS managed systems are in alignment with ISO 27001 standards, AWS has established formal policies, procedures to delineate the minimum standards for logical access to AWS resources.
IAM-02.1	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	X			SSG IT, Cloud Operations, Sales Operations, and Application Support teams remove access for any SSG employee, contractor, customer, or third-party with in 24 hours of the negotiated separation or termination date. SSG has implemented automation of notifications between all teams involved to achieve compliance.

IAM-04.1	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	X			The Cloud Operations team leverages AWS IAM management tools to track users and groups along with their level of access and privileges.
IAM-06.1	Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel only?	X			SSG restricts access to source code via the web-based version control repository application's access controls. Access is limited to developers, Cloud Operations, and employees with a documented business need.
IAM-06.2	Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only?	X			ETO provides the customer application administrators built-in tools to manage and restrict access to authorized personnel only. Customers do not have access to application source code.
IAM-08.1	Do you document how you grant and approve access to tenant data?	X			SSG's information security and privacy policies document that only employees with a business need will be granted access to customer data. SSG's technical approval process governs the approval of all access to customer data.
IAM-10.1	Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)?	X			SSG annually reviews and modifies job descriptions that document the business need for access to customer data. Cloud Operations reviews AWS IAM roles and permissions quarterly.
IAM-11.1	Is timely deprovisioning, revocation, or modification of user access to the organizations systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners, or involved third parties?	X			SSG IT, Cloud Operations, Sales Operations, and Application Support teams remove access for any SSG employee, contractor, customer, or third-party with in 24 hours of the negotiated separation or termination date. SSG has implemented automation of notifications between all teams involved to achieve compliance.
IVS-01.1	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents?	X			Systems are monitored by AWS CloudWatch and networking infrastructure is monitored by AWS Guard Duty. Alerts are automatically generated based on severity and escalation policy.

IVS-01.2	Is physical and logical user access to audit logs restricted to authorized personnel?	X			Access to logs pertaining to production systems is restricted to authorized personnel. AWS controls prevent the tampering with the logs provided.
IVS-01.5	Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	X			AWS Guard Duty automatically reviews events in the production infrastructure and alerts on security events.
IVS-03.1	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	X			System time is managed through NTP services.
IVS-07.1	Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline build standard or template?	X			Operating system hardening controls for production systems include, but are not limited to, antivirus, system level logging, AWS security groups, and CloudWatch monitoring.
IVS-08.1	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	X			Testing environments are available for clients.
IVS-08.3	Do you logically and physically segregate production and non-production environments?	X			Production and non-production environments are logically separated via AWS capabilities, i.e. network segregation, security groups, etc. Controls around physical security are inherited from our cloud hosting provider. For updated information on the control language, please see the policies linked here.
IVS-09.1	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	X			SSG implements web application firewall (WAF) technology to protect the production environments from the OWASP Top 10, malicious web attacks, and to enforce geographic access restrictions. Virtual firewalls are deployed within the environment to provide port restrictions for individual machines.

IVS-11.1	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	X			Access to the cloud administrative consoles are restricted to authorized personnel. Other SSG employees, with a documented business need, are granted read only access restricted to specific resources.
IVS-12.1	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?	X			Policies, procedures and mechanisms to protect cloud network environment are in place. Security controls are reviewed by independent external auditors during audits for SOC, PCI DSS, and ISO 27001.
IVS-12.2	Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, SNMP community strings)?	X			The ETO infrastructure is in AWS datacenters. Policies, procedures and mechanisms to protect AWS network environment are in place. AWS security controls are reviewed by independent external auditors during audits for SOC, PCI DSS, ISO 27001 and FedRAMP Authorization.
IVS-12.3	Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?	X			The ETO infrastructure is in AWS datacenters. Policies, procedures and mechanisms to protect AWS network environment are in place. AWS security controls are reviewed by independent external auditors during audits for SOC, PCI DSS, ISO 27001 and FedRAMP Authorization.
IPY-01.1	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	X			Documentation on the ETO API is maintained, and available to clients.
MOS-03.1	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores can be loaded onto a mobile device?			X	SSG does not issue mobile devices to employees. SSG's employee handbook and information security policies require BYODs to connect only to a guest network segregated from the corporate network.

SEF-02.1	Do you have a documented security incident response plan?	X			SSG has a documented security incident response policy that is reviewed by the Information Security team on an annual cadence.
SEF-02.4	Have you tested your security incident response plans in the last year?	X			SSG performs tabletops and a functional exercise of the security incident response plan annually, at a minimum.
SEF-03.1	Does your security information and event management (SIEM) system merge data sources (e.g., app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?		X		AWS CloudWatch logs host system events, access events, and security group events. AWS Guard Duty provides IDS capabilities and logs networking events for the production infrastructure. These logs are not unified under one SIEM tool, but each automatically alerts to events according to an escalation policy.
SEF-03.2	Does your logging and monitoring framework allow isolation of an incident to specific tenants?	X			Audit trails and access logs allow for the isolation of an incident to the specific customers impacted by the event.
SEF-04.4	Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	X			In the event of a legal subpoena, SSG can provide the requesting authorities the data of a single customer without exposing the data of any other customer. This is enforced by data segregation controls.
STA-02.1	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?	X			In accordance with laws and regulations, SSG provides notification, without undue delay and in no event greater than 48 hours, to affected customers in the event of a confirmed data breach.
STA-03.1	Do you collect capacity and use data for all relevant components of your cloud service offering?	X			Third-party tools are used for the tracking of use and capacity data.
STA-05.4	Do third-party agreements include provision for the security and protection of information and assets?	X			SSG requires all third-party vendors and contractors to include provisions for the security and protection of SSG and customer information before the business relationship begins.
STA-09.1	Do you permit tenants to perform independent vulnerability assessments?		X		SSG maintains accreditations and certifications performed by an independent third-party security auditing firm. SSG does not allow customers to perform independent vulnerability audits.

TVM-01.1	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your systems?	X			Systems running Microsoft Windows operating systems have antivirus installed. The antivirus is kept up to date via automatic updates, and alerts on all resolved and issues needing attention according to an escalation policy.
TVM-02.5	Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications, and systems?	X			Infrastructure management tools allow the Cloud Operations team to rapidly patch identified vulnerabilities across production systems and installed applications. Deployment mechanisms allow for the capability to rapidly patch the application. SSG IT manages patch levels through an asset management tool and provides the capability to rapidly deploy patches to all corporate endpoints.
TVM-03.1	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?			X	Production systems do not have browsers installed or use a browser that have enhanced security enabled to prevent the execution of mobile code. Use of a web browser is restricted to retrieving packages needed for the application.
TVM-03.2	Is all unauthorized mobile code prevented from executing?	X			Production systems do not have browsers installed or use a browser that have enhanced security enabled to prevent the execution of mobile code.

DOCUMENT HISTORY

Date	Description
June 2020	Document Template Updated
May 2020	Document Updated
January 2020	Document Updated
December 2019	Document Created