CITY OF SAN ANTONIO
INFORMATION TECHNOLOGY SERVICES DEPARTMENT

Cloud Security Assessment Questionnaire

for Vendors(Amazon Web Services -AWS)

03/08/2023

Table of Contents

Overview

This document will be used as a preliminary questionnaire to allow Information Technology Services Department (ITSD) Security Group to assess the physical, logic and security administration controls used by a third party application service provider or business partner.

Assessment Process

Identification of Parties Involved

The following are the four groups involved in this assessment process:

Group Name	Role
ITSD Security	Initiator of Process, Performs Assessment, Reports Findings/Risk Recommendation
Project Manager	Coordinates interaction between ITSD and external vendors.
-Vendor/Company-	Provides answers to questionnaire.
CSO	Makes Risk Recommendation
Business Owner	Accepts Final Report

Area 1	Certifications, Programs, Reports, and Third-Party Attestations	
01	AWS GovCloud? What Region of GovCloud? (AWS GovCloud (US-West) or AWS GovCloud (US-East)	(Select One)
02	Project is associated with CJIS, PCI or HIPAA Data?	(Select One)
03	What Type of VPN Connection established with AWS (Ex AWS Site-to-Site VPN, AWS Client VPN, AWS VPN Cloud-Hub, Third party software VPN appliance and AWS Direct Connect)	(Select One)
04	How many COSA users are configured AWS (IAM) ?	(Select One)
05	Azure Active Directory Integration Single Sign On and user provisioning"	(Select One)
06	Who is responsible for Monitoring VPN Connection and do we have access to see Amazon VPC Dashboard (VPN tunnel status, Site-to-Site VPN connections)?	(Select One)
07	Vendor signed with AWS CloudTrail & AWS Cloud watch?	(Select One)
08	How much assistance will the vendor provide COSA with investigations if there is a security breach such as an unauthorized disclosure of my data, or if there is a need to perform legal electronic discovery of evidence?	(Select One)

Area 2	Select the Security, Identity, & Compliance Tools Implemented for the Project		Response
09	AWS Identity and Access Management	(Identity and Access Control)	(Select One)
10	AWS Artifact	Security and compliance documents (AWS ISO certifications, PCI, and SOC).	(Select One)
11	Amazon Cognito	(User pools and identity pools)	(Select One)
12	Amazon Detective	(Identify the root cause of security findings or suspicious activities)	(Select One)
13	AWS Directory Service	(Identity and Access Control)	(Select One)
	AWS Firewall Manager		(Select One)
14	AWS Cloud Directory		(Select One)
15	AWS Cloud Trail	(Monitoring and Logging)	(Select One)
16	Amazon Cloud Watch	(Monitoring and Logging)	(Select One)
17	Amazon GuardDuty	(Monitoring and Logging)	(Select One)
18	Amazon Inspector		(Select One)
19	Amazon Macie		(Select One)
20	AWS Resource Access Manager		(Select One)
21	AWS Secrets Manager		(Select One)
	AWS Security Hub		(Select One)
	AWS Shield		(Select One)
22	AWS Single Sign-On	(Identity and Access Control)	(Select One)
	AWS WAF		(Select One)

Specify any other Security Tools Integrated with AWS Cloud:

Area 3	HOSTED WEB OR CLOUD APPLICATION	Response
1	Will the services provided to COSA include Data-as-a-Service (DaaS)? *Data is provided to COSA through specific interfaces.*	(Select One)
2	Will the services provided to COSA include Software-as-a-Service (SaaS)? *COSA uses your applications running on your cloud infrastructure.*	(Select One)
3	Will the services provided to COSA include Platform-as-a-Service (PaaS)? *COSA deploys onto your cloud infrastructure COSA-created or acquired applications created using programming languages, libraries, services, and tools supported by you.*	(Select One)
4	Will the services provided to COSA include Infrastructure-as-a-Service (IaaS)? *COSA is able to deploy and run arbitrary software, which can include operating systems and applications, on processing, storage, networks, and other fundamental computing resources you provide.*	(Select One)
5	Does the application support per-client security controls:	(Select One)
6	Password complexity requirements?	(Select One)
7	Password length requirements?	(Select One)
8	Password expiration?	(Select One)
9	Password history requirements?	(Select One)
10	Account lockout due to failed access attempts? (maximum of six)	(Select One)
11	Are passwords masked while entered?	(Select One)
12	Do you provide tenants with strong (multifactor) authentication options (digital certs, tokens, biometric, etc.) for user access?	(Select One)
13	Can the application login screen be restricted to the COSA network IP range?	(Select One)
14	Does the application require transport encryption? (SSL)	(Select One)
15	Has the application been inspected for Cross-Site Scripting attacks?	(Select One)
16	Have identified Cross-Site Scripting vulnerabilities been remediated?	(Select One)
17	Has the application been inspected for database injection attacks?	(Select One)
18	Have identified database injection vulnerabilities been remediated?	(Select One)
19	Has the application been inspected for session hijacking attacks?	(Select One)
20	Have identified session hijacking vulnerabilities been remediated?	(Select One)
21	Has the application been inspected for buffer overflow attacks?	(Select One)
22	Have identified buffer overflow vulnerabilities been remediated?	(Select One)
23	Does the application validate user input fields against malicious data entry?	(Select One)
24	Does the application restrict storing sensitive data on end client workstations? (cookies)	(Select One)
25	Does the application restrict account administration through the website?	(Select One)
26	Does the application restrict system administration through the website?	(Select One)
27	Has the application been cleansed of built-in sample application code? (scripts)	(Select One)
28	Has the application been cleansed of built-in sample data?	(Select One)
29	Is application security assessed on a periodic basis?	(Select One)

Area 3	HOSTED WEB OR CLOUD APPLICATION	Response
30	Is the assessment performed by an external security consultant or company?	(Select One)
31	Is the assessment performed annually?	(Select One)
32	Is a security assessment performed after major upgrades to the application?	(Select One)
33	Are issues identified by a security assessment remediated?	(Select One)
34	Do you have the ability to logically segment customer data so that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	(Select One)
35	Can you provide the physical location of storage of a tenant's data upon request?	(Select One)
36	Do you allow tenants to define acceptable geographical locations for data routing or data storage?	(Select One)
37	Do you have technical control capabilities to enforce tenant data retention policies?	(Select One)
38	Do you have controls in place to prevent data leakage (intentional/accidental compromise) between tenants in a multi-tenant environment?	(Select One)
39	Can you provide a documented procedure on how tenant data is sanitized from your systems once the service contract/relationship ends?	(Select One)
40	Do you "data mine" tenant data for your company's benefit?	(Select One)
41	If yes, do you provide tenants the ability to opt-out?	(Select One)
	Additional Information:	