CITY OF SAN ANTONIO
INFORMATION TECHNOLOGY
SERVICES DEPARTMENT

Cloud Security Assessment Questionnaire for Vendors (Microsoft Azure)

Version 4.0 07/01/2020

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**	
1.	Azure GovCloud? What Region of GovCloud? (US Gov Arizona, Texas or Virginia)	(Select One)
2.	Project is associated with CJIS, PCI or HIPAA Data?	(Select One)
3.	What Type of virtual network is created with Azure (Ex: Portal, PowerShell or Azure CLI)	(Select One)
4.	Who is responsible "Security controls for Azure VPN Gateway and Azure Vnet"? (ex-tools: Azure Monitor Log Analytics; Azure VPN Gateway metrics) COSA or Vendors?	(Select One)
5.	COSA users are configured Azure Active Directory (IAM)?	(Select One)
6.	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
7.	Azure Identity and Access Management (Identity and Access Control) Azure AD	(Select One)
8.	Azure Firewall	(Select One)
9.	Azure DDoS Protection	(Select One)
10.	Azure NetApp Files	(Select One)
11.	Azure Network-based anomaly detection	(Select One)
12.	Azure adaptive application controls	(Select One)
13.	Azure Web filtering	(Select One)
14.	Microsoft Endpoint Protection for Azure	(Select One)
15.	Azure Vulnerability management (Qualys Scanner)	(Select One)
16.	**Specify any other Security Tools Integrated with Azure 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.	Can the application login screen be restricted to the COSA network IP range?	(Select One)
13.	Does the application require transport encryption? (SSL)	(Select One)
14.	Has the application been inspected for Cross-Site Scripting attacks?	(Select One)
15.	Have identified Cross-Site Scripting vulnerabilities been remediated?	(Select One)
16.	Does the application restrict storing sensitive data on end client workstations? (cookies)	(Select One)
17.	Does the application restrict account administration through the website?	(Select One)
18.	Is application security assessed on a periodic basis?	(Select One)

Area 3	HOSTED WEB OR CLOUD APPLICATION	Response
1.	Is the Security assessment performed by an external security consultant or company?	(Select One)
2.	Is the Security assessment performed annually?	(Select One)
3.	Is a security assessment performed after major upgrades to the application?	(Select One)
4.	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)
5.	Do you have technical control capabilities to enforce tenant data retention policies?	(Select One)
6.	Do you have controls in place to prevent data leakage (intentional/accidental compromise) between tenants in a multi-tenant environment?	(Select One)
7.	Do you “data mine” tenant data for your company’s benefit?	(Select One)
8.	If yes, do you provide tenants the ability to opt-out?	(Select One)
	Additional Information:	