Critical Customer Factors

# Objectives:

* Production ready Single sign-on with Office 365
* Secure network design using layers of security
* Billing Structure for categorizing cloud computing spending across the enterprise.
* Separation of managed and sandbox workloads
* Secure and Application Lifecycle Management roles.
* Identity services, which will give a foundation for establishing robust applications in the cloud
* Operational excellence with monitoring and alerting

# Scope

## Pre Requisites

Customer will provide:

1. Azure Enrollment with Enterprise Administrator Access and Global Administrator access
2. Class B IP address to be subdivided with four Azure regions
3. VPN Gateway IP address and/or ExpressRoute Service Provider with BGP Neighbor Address and either Private or Public ASN number(s)
4. Stakeholders for Network, Security, Operations, Identity and System Administration to participate in an Interview process.

|  |  |
| --- | --- |
| Project/Work stream | Description |
| Azure Enrolment Governance | * Comprehensive planning activities to design your organization’s Subscription, administrative, naming convention, information security, and billing models. * Deploy Financial and Security Model * Deploy up to 2 Departments[[1]](#footnote-1)[1] in Enterprise Portal (https:/ea.azure.com) * Deploy up to 2 Accounts[[2]](#footnote-2)[2] per Department in the Enterprise Portal. (managed and sandbox) * Detailed design of a base networking, storage, identity and compute infrastructure in your Azure subscription model based on a Class B IP pattern across four Azure regions * Deploy up to 5 subscriptions in each of the Managed Department’s Accounts.   + Production, the services that are expected to be up and hosted with an availability expectation.   + CIJS or HBI, for any data that is exchanged between public safety organizations with compliance requirements outlined by the FBI. Or for non-public safety organizations the use of High Business Impact systems that may require background checks or security clearance.   + Pre-Production, services that are used for application lifecycle management purposes, such as testing and development.   + Storage, for services that are hybrid storage centric such as StorSimple, on premise Backup and Recovery Services, Azure File Services.   + Services, a special subscription with restrictions to protect data that is highly sensitive, yet requires access to or from multiple external resources.  This subscription also holds the central network routing gateways for the other subscriptions to peer with for accessing hybrid networking functionality with the customer premise. For example, Identity Services like Domain Controllers, Express Route Gateways, VPN Gateways. * The configuration of the Azure Virtual network for each subscription, following a pattern that is outlined consistently and deployed using a script, including: * Class B IpV4 network configuration of Subnets for the DMZ, Web, Application, Database tiered workloads. * Network Security Groups that have default rules that shape network traffic to standards, specifically, a Deny rule for subnets besides the Allow DMZ subnets will be allowed to have Internet endpoints to receive traffic. * Two sites, to enable georedundant requirements between Community Cloud locations. * Local Network definitions, ExpressRoute and VPN connections between the Subscriptions and their peer network in the alternate data center, the Agency’s Premise, and the local datacenter’s Services Subscription (for Identity and other communications) * Provide informal knowledge transfer to your staff to prepare them to operate the Solution and to expand Microsoft Azure usage into other scenarios |
| Secure and HA Cloud Identity | * Deploy a seven server Identity Pattern that will enable the Agency to promote two Domain Controllers and integrate them with their Office 365 subscription using AAD Connect and ADFS in a secure configuration that is also highly available. * Deploy two Microsoft Server 2012 R2 (or greater) Web Application Proxy (WAP) servers in the DMZ subnet of each Agency’s “Services” subscription, with: * A public endpoint for port 443 which will receive the authentication request for the Agency’s DNS Tenant. * Configure with static IP addresses in the DMZ subnet. * Configure the Microsoft Windows Server Active Directory Federation Server (ADFS) Proxy service * Deploy two Microsoft Server Active Directory Domain Services (ADDS) Servers in the Services Subnet * Configure static IP addresses for each server * Note, the Agency will be responsible for:   + performing the Domain Controller promotion to maintain separation of duties.   + Add the ADFS servers to the domain.   + Add the AAD Connect Server to the domain. * Deploy two Microsoft Server Active Directory Federation Servers in the Services Subnet * Configure an internal network load balancer with a static IP address * Deploy the AAD Connect Server and run the configuration script to enable SSO for the Agency’s Office 365. |
| AzureFoundation Network Pattern | * Deploy five VNETs across four Azure Regions * Configure VNET Peering from workload VNETs (Prod, HBI/CJIS, PreProd, Storage) with the hub VNET (Services). * Configure Active/Active ExpressRoute Gateway with an ExpressRoute Circuit * Configure Active/Active VPN Gateway * Configure Connections between the Four Azure Regions selected and up to two Azure Peering locations and two Customer premise locations. * Test the failover of the Active/Active routing to show there are no single points of failure. |
| [Optional] Azure Proof-of-Concept Workload Migration | Plan, build, test, and deploy a Solution consisting of **one** application workload to Microsoft Azure |
| [Optional] Azure Policy using the Azure scaffolding | The Azure Scaffolding pattern is in development to enforce all the NSGs or Naming Conventions or??? |

## Out of Scope

Configuring on premise network devices. The goal of the solution is to have all routing be dynamic routing.

1. [1] A Department is a financial boundary in the Azure Enterprise Portal.  There is a Department Administrator that controls the costs of the Department’s Accounts. [↑](#footnote-ref-1)
2. [2] An Account is a financial boundary in the Azure Enterprise Portal that has a relationship to [↑](#footnote-ref-2)