Current State

People and Process

- What industry is the organization in? Briefly describe the organization.

- What is the organizational structure for IT? Describe the various departments and the reporting structure up to the C-level.

- How are roles and responsibilities distributed in the IT teams? Have they been adapted to cloud consumption? Does a RACI exist for cloud?

- Does the organization have a cloud strategy? If so, briefly describe it.

- What laws and regulations are the organization subject to? Has the organization adopted any control frameworks such as CIS or NIST?

- Has the organization created a Cloud Center of Excellence (CCoE)?

- Has the organization decided upon naming standards or tagging schemes for cloud resources?

- What is the chargeback model the organization has decided upon?

- Does the organization have an active Enterprise Enrollment? Has it made any Azure commitments?

- Has the organization created any Azure Accounts? What about Azure Subscriptions? If so, what type of subscriptions has it created? Does it have a standardized process for creation of Azure Subscriptions?

- Describe at high level how the customer does business with its customers (B2B and consumers) and what role technology plays there.

- In which functions does the customer engage (or has engaged in the past) partners/SIs/MSPs?

Technology

- How many physical locations does the organization have? Describe its physical presence including number of headquarters, supporting offices, branches, data centers, and colocations. Include the geographical distribution of the physical locations and the operators of any colocations in use.

- How are the physical locations connected with each other (MPLS, IPSec VPN over the Internet, etc)? Who is the ISP for the connections? What are the speeds of the connections? Is there redundancy and failover to the connections such as multiple ISPs?

- How does the organization connect to the Internet? Who is the ISP? What speed is the connection? Is there redundancy in providers or physical connections?

- How is asset management performed today? Do you have a configuration management database (CMDB)? What solution is used?

- How is service request management handled today? How is change management handled? How is incident management handled? What solutions are in place? Are these solutions running on-premises or are they SaaS offerings?

- What physical hardware is in use in the data centers? Describe the hardware used for compute, storage, and network including the manufacturers.

- What security appliances are in use in the data center? Describe the appliances including manufacturer and model numbers if possible. What capabilities are each of these devices providing?

- How is the environment segmented? Is classic segmentation at layer four with a DMZ and Trusted network? Zero Trust? Microsegmentation? A combination? Is there segmentation at the physical layer of environments?

- What hypervisors are in use? What operating systems are in place? What versions or flavors?

- How are core infrastructure services handled?
    - How is DNS resolution handled for internal resources? Where are internal DNS zones hosted? Where are external DNS zones hosted?
    - How is IPAM handled?
    - How is NTP provided?
    - How is PKI handled internally? Externally?
    - How is key management handled? Are HSMs used? If so, what make and model?
    - Are there load balancers in use? If yes what is the make and model? Are these operating at layer 4 or layer 7? Is there geo-load balancing being used?
    - Are there any API Gateways in use? If so, what vendor is being used?

- How is identity management handled at the organization?
    - Is there an identity management solution in place (MIM, SailPoint, Ping, etc)?
    - What identity repositories are in place (OpenLDAP, Windows AD, Azure AD, Mainframe (ACF2) local user database, etc)?
    - Is there a modern identity solution in place that provides modern authentication such as SAML, Open ID Connect, OAuth (AD FS, Ping, Okta, etc)?
    - Is there a privileged management solution in place? If so how is it being used (privileged session management, password vaulting, application credential storage, etc)?

    - Is there MFA in use with the organization? What is the form factor? (Smartcard, NFC, usb token, OTP, etc)
    - Is there is an access management system in place? (i.e. Siteminder, Ping, ISAM, F5 APM, etc)

- If Windows Active Directory is in place, describe the structure including number of forests, domains, trusts, domain controllers per domain, and Active Directory site structure. Include a brief description of the purpose of the forests, domains, and trusts.

- If an Azure Active Directory tenant has been setup describe the number of tenants, how identities are synced, how authentication occurs (password hash sync (PHS), AD FS, passthrough authentication (PTA), third party security token service (STS)), how privileged access is handled, and whether it's used as identity source for third party SaaS offerings.

- What monitoring solutions are in place for network, application, synthetic transaction, and compute?

- What does the organization do for logging? What are the retention requirements for logs and does it differ with types of logs, such as operational vs security? Does it use a SIEM? If so which one? Is the SIEM used for both security operations AND standard operations?

- What solution does the organization use for source control? Has it established a CI/CD pipeline? If so, what product(s) is it using for the CI/CD pipeline?

- Is the pipeline used for just application code or is it also used for infrastructure?

- What does a typical application stack look like at your organization? (Commercial off the shelf, LAMP, .NET, etc)

- What application databases are in use? (MS SQL, Oracle, MySQL, etc)

- Does the organization have a big data workloads or strategy? What products are in use?

- What solution does the organization use for configuration management and security baseline of Microsoft Windows? What about non-Microsoft operating systems?

- What solution does the organization use for patching and updates?

- What solution is in place for backups? Do you have retention requirements? What about disaster recovery? Does the organizational regularly validate disaster recovery processes and procedures?

- How does the organization separate dev, non-production, and production?

- Describe the organization’s Microsoft Azure usage if it is already being used.
    - Examples areas to explore:
        - Has a management group and subscription model been defined?
        - Is Azure Policy being used?
        - Have RBAC roles been defined and created?
        - What regions are being used?
        - How does the organization connect to Azure?
        - Has a network topology been defined?
        - How is logging being handled?
        - How is disaster recovery and backup being handled?
        - What products are in use and how?
        - What workloads are in place?