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

- What laws and regulations is 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 organized decided upon naming standards or tagging schemes for cloud resources?

- 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?

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? What solution is used?

- How is request management handled today? 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 provided for internal zones? External zones?
  - 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?

- 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 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)?

- If Windows Active Directory is in place, describe the structure including number of forests and domains, number of trusts, and Active Directory site structure.

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

- What monitoring solutions are used within the organization?

- What does the organization do for logging? Does it use a SIEM? If so which one?

- What solution does the organization use for source control? Has it established a CI/CD pipeline?

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

- What solution does the organization use for configuration management of Microsoft Windows?

- What about non-Microsoft operating systems? Third-party applications?

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

- What solution is in place for backups? What about disaster recovery?

- How does the organization separate Dev, QA, 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?
    - Has a network topology been defined?
    - How is logging being handled?
    - How is disaster recovery and backup being handled?
    - What products are in used and how?
    - What workloads are in place?