Azure Foundation Onboarding Assessment



Questionnaire Guidelines

Prepared for

[Type Customer Name Here]

2/8/2022

Version Draft

Prepared by

**[Type Author Name Here]**

Contributors

**[Type Contributors Here]**

Contents

[1 Introduction 4](#_Toc84246613)

[2 Enterprise Agreement (EA) enrollment and Azure Active Directory tenants 9](#_Toc84246614)

[3 Identity and Access Management 27](#_Toc84246615)

[3.1 Assessment details 27](#_Toc84246616)

[3.2 Additional findings and Recommendations 47](#_Toc84246617)

[4 Management Group and Subscription Organization 48](#_Toc84246618)

[4.1 Assessment details 48](#_Toc84246619)

[4.2 Additional findings and Recommendations 66](#_Toc84246620)

[5 Network Topology and Connectivity 67](#_Toc84246621)

[5.1 Assessment details 67](#_Toc84246622)

[5.2 Additional findings and Recommendations 95](#_Toc84246623)

[6 Management and Monitoring 96](#_Toc84246624)

[6.1 Assessment details 96](#_Toc84246625)

[6.2 Additional findings and Recommendations 119](#_Toc84246626)

[7 Business Continuity and Disaster Recovery 120](#_Toc84246627)

[7.1 Assessment details 120](#_Toc84246628)

[7.2 Additional findings and Recommendations 131](#_Toc84246629)

[8 Security, Governance, and Compliance 132](#_Toc84246630)

[8.1 Assessment details 132](#_Toc84246631)

[8.2 Additional findings and Recommendations 168](#_Toc84246632)

[9 Platform Automation and DevOps 169](#_Toc84246633)

[9.1 Assessment details 169](#_Toc84246634)

[9.2 Additional findings and Recommendations 194](#_Toc84246635)

1. Introduction

This document is delivered to [Type Customer Name Here] to detail the gaps, findings and recommendations identified during the CAF Landing Zone Assessment phase, prior CAF Landing Zone Design Workshop.

1. Engagement Overview

[Type Customer Name Here] has engaged Microsoft to assess the current state to identify whether Contoso is ready for CAF Landing Zone Design Workshop and Implementation based on Cloud Adoption Framework for Azure Enterprise Scale Landing zones.

The objectives of this engagement and this document are the followings:

* Understand Contoso’s current environment and readiness to move to Azure and plan for Enterprise Scale.
* Deep understanding of Contoso’s Azure environment, workloads, and technical constraints.
* Identify technology gap and help to build a roadmap to achieve the desired goal.
* Provide input of customer’s current situations and requirements to use as next steps in the program.
* Identify candidate Landing Zones for applications in Azure.
* Gather required information to build Enterprise-scale architecture in compliance with your requirements (next phases).
* Qualify whether the customer is ready for design workshop and implementation phases within CAF Landing Zone.

1. Enterprise Scale Landing Zones

Azure landing zones are the output of a multi-subscription Azure environment that accounts for scale, security, governance, networking, and identity. Azure landing zones enable application migrations and greenfield development at an enterprise scale in Azure. These zones consider all platform resources that are required to support the customer's application portfolio and don't differentiate between infrastructure as a service or platform as a service.

* 1. Design Principles

The enterprise-scale architecture prescribed in this guidance is based on the design principles described here. These principles serve as a compass for subsequent design decisions across critical technical domains. Familiarize yourself with these principles to better understand their impact and the trade-offs associated with nonadherence.

* + 1. Subscription democratization

Subscriptions should be used as a unit of management and scale aligned with business needs and priorities to support business areas and portfolio owners to accelerate application migrations and new application development. Subscriptions should be provided to business units to support the design, development, and testing of new workloads and migration of workloads.

* + 1. Policy-driven governance

Azure Policy should be used to provide guardrails and ensure continued compliance with your organization's platform, along with the applications deployed onto it. Azure Policy also provides application owners with sufficient freedom and a secure unhindered path to the cloud.

* + 1. Single control management plane

Enterprise-scale architecture shouldn't consider any abstraction layers, such as customer-developed portals or tooling. It should provide a consistent experience for both AppOps (centrally managed operation teams) and DevOps (dedicated application operation teams). Azure provides a unified and consistent control plane across all Azure resources and provisioning channels subject to role-based access and policy-driven controls. Azure can be used to establish a standardized set of policies and controls for governing the entire enterprise estate.

* + 1. Application-centric and archetype-neutral

Enterprise-scale architecture should focus on application-centric migrations and development rather than pure infrastructure lift-and-shift migrations, such as moving virtual machines. It shouldn't differentiate between old and new applications, infrastructure as a service, or platform as a service application. Ultimately, it should provide a safe and secure foundation for all application types to be deployed onto your Azure platform.

* + 1. Align Azure-native design and roadmaps

The enterprise-scale architecture approach advocates using Azure-native platform services and capabilities whenever possible. This approach should align with Azure platform roadmaps to ensure that new capabilities are available within your environments. Azure platform roadmaps should help to inform the migration strategy and enterprise-scale trajectory.

* 1. Critical Design Areas

Each Azure landing zone implementation option provides a deployment approach and defined design principles. The objectives of each design area are listed in the following table:

|  |  |  |
| --- | --- | --- |
| Design Areas | Objectives | Relevant methodologies |
| Enterprise enrollment | For enterprise customers with an Azure commitment, proper tenant creation and enrollment is an important early step. | Ready |
| Identity | Identity and access management is a primary security boundary in the public cloud. It's the foundation for any secure and fully compliant architecture. | Ready |
| Network topology and connectivity | Networking and connectivity decisions are an equally important foundational aspect of any cloud architecture. | Ready |
| Resource organization | As cloud adoption scales, considerations for subscription design and management group hierarchy have an impact on governance, operations management, and adoption patterns. | Govern |
| Governance disciplines | Automate auditing and enforcement of security, governance, and compliance policies. | Govern |
| Operations baseline | For stable, ongoing operations in the cloud, an operations baseline is required to provide visibility, operations compliance, and protect and recover capabilities. | Manage |
| Business continuity and disaster recovery (BCDR) | Resiliency is key for smooth functioning of applications. BCDR is an important component of resiliency. BCDR involves protection of data via backups and protection of applications from outages via disaster recovery. | Manage |
| Deployment options | Align the best tools and templates to deploy your landing zones and supporting resources. | Ready |

* 1. Cloud Adoption Framework Azure Landing Zones

The enterprise-scale architecture represents the strategic design path and target technical state for your Azure environment. It will continue to evolve alongside the Azure platform and is defined by the various design decisions that your organization must make to map your Azure journey.

Not all enterprises adopt Azure in the same way, so the Cloud Adoption Framework for Azure enterprise-scale landing zone architecture varies between customers. The technical considerations and design recommendations of the enterprise-scale architecture might lead to different trade-offs based on your organization's scenario. Some variation is expected, but if you follow the core recommendations, the resulting target architecture will set your organization on a path to sustainable scale.

* 1. Prescriptive Guidance

The enterprise-scale architecture provides prescriptive guidance coupled with Azure best practices. It follows design principles across the critical design areas for an organization's Azure environment.

* 1. Qualifiers: Should I start with enterprise scale?

The enterprise-scale architecture is modular by design. It allows you to start with foundational landing zones that support your application portfolios, no matter whether the applications are being migrated or are newly developed and deployed to Azure. The architecture can scale alongside your business requirements regardless of scale point.

* 1. Start with a Cloud Adoption Framework Azure Landing Zone

The enterprise-scale approach to construct landing zones includes three sets of assets to support cloud teams:

[Design guidelines](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/design-guidelines): Guide to the critical decisions that drive the design of the Cloud Adoption Framework for Azure enterprise-scale landing zone.

[Architecture](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/architecture): Conceptual reference architecture that demonstrates design areas and best practices.

[Implementations](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/implementation): Azure Resource Manager template of the architecture to accelerate adoption.

* 1. Document Purpose

The purpose of this document is to detail the identified gaps and recommendations during the Assessment week. Its content is based on information gathered during the customer interviews and participatory whiteboarding sessions that was conducted with [Type Customer Name Here] on [Date of the discovery week].

* 1. Intended Audience

This document is intended for the [Type Customer Name Here] is the following teams:

* Technical and business decision makers
* Architect Lead/Chief Architect
* Networking team (NetOps)
* Identity and Access Management team (IAM)
* Systems (SysOps: OS, DB)
* Operations and Management team
* Security (SecOps)
* DevOps and Automation teams
* Application Architecture team

It assumes a working knowledge of Azure Infrastructure, Governance, Identity, Networking Security, Monitoring and DevOps.

1. Enterprise Agreement (EA) enrollment and Azure Active Directory tenants

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Label | Question | Answer | Why consider this | Suggested Actions | Learn More |
| **EA01** | **How are you using Azure in terms of Billing?** |  | The enterprise enrollment defines the shape and use of Azure services within your company from a contractual point of view. Within the enterprise agreement, you can further subdivide the environment into departments, accounts, and finally, subscriptions and resource groups to match your organization's structure. Use Azure from Enterprise Agreement to avoid Shadow IT across the organization. | Consume Azure services through Enterprise Agreement for Billing purposes and avoid Shadow IT.  Only use the authentication type Work or school account for all account types. Avoid using the Microsoft account (MSA) account type.  Assign a budget for each account, and establish an alert associated with the budget.  An organization can have a variety of structures, such as functional, divisional, geographic, matrix, or team structure. Use organizational structure to map your organization structure to your enrollment hierarchy.  Create a new department for IT if business domains have independent IT capabilities.  Restrict and minimize the number of account owners within the enrollment to avoid the proliferation of admin access to subscriptions and associated Azure resources.  If multiple Azure Active Directory (Azure AD) tenants are used, verify that the account owner is associated with the same tenant as where subscriptions for the account are provisioned.  Set up Enterprise Dev/Test and production environments at an EA account level to support holistic isolation.  Don't move or rename an EA account in Azure AD.  Periodically audit the EA portal to review who has access and avoid using a Microsoft account where possible.  Provision Azure Subscription automatically through Service Principals when is needed. | Enterprise Agreement enrollment and Azure Active Directory tenants  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/enterprise-enrollment-and-azure-ad-tenants  Microsoft Azure EA Sponsorship  <https://azure.microsoft.com/en-us/offers/ms-azr-0136p/>  Get started with the Azure Enterprise portal  <https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/ea-portal-get-started> |
|  |  | We use Azure Enterprise Agreement, but we also have some pay as you go subscriptions. We may have some unmanaged subscriptions below EA or as pay as you go. |  |  |  |
|  |  | We are using Azure through EA. Departments are tied to budgets and Account Admins manage their own billing. Few people in the organization can create subscription through Azure / EA portals when it is needed.  Custom detaills: |  |  |  |
|  |  | We are using Azure through EA. Departments are tied to budgets and Account Admins manage their own billing. We have automated mechanism to provision subscriptions under EA agreement through Service Principals. |  |  |  |
| **EA02** | Are notifications set up on the Enterprise Agreement Portal? |  | Enterprise Administrators are automatically enrolled to receive usage notifications associated to their enrollment. Each Enterprise Administrator can change the interval of the individual notifications or can turn them off completely. If EA Admin Accounts mailboxes are unattended, you may miss important notifications from EA.  Notification contacts are shown in the Azure EA portal in the Notification Contact section. Managing your notification contacts makes sure that the right people in your organization get Azure EA notifications.  Notification contacts are entered by enterprise administrators. You need only to provide an email address that can receive day to day emails; there is no need to use the organization account.  Receive usage notifications for the agreement.  Receive Azure service update notifications. | Don't ignore notification emails sent to the notification account email address. Microsoft sends important EA-wide communications to this account.  Set up the notification contact email address to ensure notifications are sent to an appropriate group mailbox. | Azure EA portal administration  https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/ea-portal-administration    Roles in the Enterprise Portal  https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/understand-ea-roles    Enterprise Agreement enrollment and Azure Active Directory tenants  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/enterprise-enrollment-and-azure-ad-tenants |
|  |  | Notification contact email address is setup for users in EA, but we are not sure who receives these notifications and what action they can when they receive the email. |  |  |  |
|  |  | Notification contact email address is setup for a group in EA. We do not have a formal process to manage the notification. |  |  |  |
|  |  | We redirect EA notification to **specific** DL in the organization and act based on the notification through change management. |  |  |  |
| **EA03** | What is the Authentication level in the EA? |  | Manage EA level authentication and access through own Azure AD tenant and maintain control over identities with high privilege. | Only use the authentication type Work or school account for all account types. Avoid using the Microsoft account (MSA) account type. If Microsoft Account used, convert MSA or Live ID account to Work or School Accounts:  Azure Enterprise users can convert from a Microsoft Account (MSA or Live ID) to a Work or School Account (which uses Active Directory in Azure) authentication type.  Add the work or school account to the Azure EA Portal in the role(s) needed.  If you get errors, the account may not be valid in the active directory. Azure uses User Principal Name (UPN), which isn't always identical to the email address.  Authenticate to the Azure EA portal using the work or school account.  Review and document all Account Owners and Service Administrators across all subscriptions.  Plan and implement for emergency access or break-glass accounts to prevent tenant-wide account lockout. | Azure EA portal administration  https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/ea-portal-administration  Troubleshoot Azure EA portal access  https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/ea-portal-troubleshoot  Enterprise Agreement enrollment and Azure Active Directory tenants  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/enterprise-enrollment-and-azure-ad-tenants  Manage emergency access accounts in Azure AD  https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-emergency-access |
|  |  | We have several users as Enterprise Administrator in the EA including some legacy administrators who previously were managing the EA. The Authentication level is mixed and there are some Microsoft Accounts among the EA Admins. |  |  |  |
|  |  | We only have Work/School account in the EA as admins, however currently EA the authentication level is setup as mixed. Not sure what account is set as the existing subscriptions' Service admins/ Account owners. |  |  |  |
|  |  | EA authentication level is Work/School Account, and we have setup an emergency accounts as cloud only users from our Azure AD tenant. In all subscriptions Service Admins / Account owners are known and documented. |  |  |  |
| **EA04** | Are there procedures in places to review/audit who has access to the EA portal? |  | Enterprise Agreement portal has various administrator roles and the operation permissions in the portals. It is important to make sure right people are granted with these roles:  Enterprise administrator:  Enterprise administrators have the highest level of access permissions. They can:  Manage accounts and account owners.  Manage enterprise administrators.  Manage department administrators.  Manage notification contacts.  View usage for all accounts.  View unbilled charges for all accounts.  A single Enterprise Agreement can have multiple enterprise administrators.  All enterprise administrators inherit the role of department administrator.  Department administrators:  Create and manage departments.  Create new account owners.  View detailed usage information for the department that they manage.  View costs (if granted the necessary permissions).  A single Enterprise Agreement can have multiple department administrators.  Account owners:  Create and manage subscriptions.  Manage service administrators.  View subscription usage.  Every account must have a unique organization account.  Service administrators:  Sign in to the: Azure portal  Access and manage subscriptions and development projects in the Developer Portal.  An organization account may be used in different subscriptions and hierarchy levels. | Periodically audit the EA portal to review who has access and avoid using a Microsoft account where possible. | Roles in the Enterprise Portal  https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/understand-ea-roles  Enterprise Agreement enrollment and Azure Active Directory tenants  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/enterprise-enrollment-and-azure-ad-tenants |
|  |  | We are not aware of who has access to the EA portal. |  |  |  |
|  |  | There are no procedures in place to regularly review who has access to the EA portal and/or there are MSA accounts that have access to the EA portal. |  |  |  |
|  |  | There are procedures in place to regularly review who has access to the EA portal and there are no MSA accounts that have access to the EA portal. |  |  |  |
| **EA05** | Do you require MFA for EA admins when they login to EA portal? |  | MFA provides a second barrier of authentication adding another layer of security. It is recommended to enforce MFA and conditional access policies for all privileged accounts to make it more secure. MFA does provide another barrier of authentication but does not stop phishing or social engineering such as hacker taking physical possession of your phone or Sim Swapping or cloning. It is recommended that MFA should be implemented with device management policy (such as strong pin locking and encryption and erasing device remotely when its lost). Out of band multifactor authentication (such as biometric) is also consider secure form of MFA.  Organizations want to minimize the number of people who have access to secure information or resources, because that reduces the chance of a malicious actor getting that access, or an authorized user inadvertently impacting a sensitive resource. However, users still need to carry out privileged operations in Azure AD, Azure, Microsoft 365, or SaaS apps. Organizations can give users just-in-time privileged access to Azure resources and Azure AD. There is a need for oversight for what those users are doing with their administrator privileges. | Enforce multi-factor authentication and conditional access policies for all privileged accounts for greater security.  Use Multi-factor authentication from Azure AD conditional Access to Admins group and AAD roles. Exclude Break Glass Accounts from Conditional Access Policy.  Use Azure AD Privileged Identity Management for identity and access management. | What is Conditional Access?  https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview  What is Azure AD Privileged Identity Management?  https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure  Enterprise Agreement enrollment and Azure Active Directory tenants  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/enterprise-enrollment-and-azure-ad-tenants |
|  |  | Some Admins may require using MFA, but it is not mandated for all EA admins. |  |  |  |
|  |  | We have setup a policy to enforce MFA for any EA admins and restrict access based on risky sign ins or users. |  |  |  |
|  |  | We have setup a policy to enforce MFA for any EA admins and restrict access based on risky sign ins or users. We have a separated account for privileged account than day to day job, but notifications from EA are monitored. |  |  |  |
| **EA06** | Is the hierarchy and relationship between the Azure Enterprise Enrollment, the departments, the Azure accounts, and the subscriptions defined? |  | The enrollment provides a hierarchical organizational structure to govern the management of subscriptions.  Multiple environments can be separated at an EA-account level to support holistic isolation.  There can be multiple administrators appointed to a single enrollment.  Each subscription must have an associated account owner.  Each account owner will be made a subscription owner for any subscriptions provisioned under that account.  A subscription can belong to only one account at any given time.  A subscription can be suspended based on a specified set of criteria. | An organization can have a variety of structures, such as functional, divisional, geographic, matrix, or team structure. Use organizational structure to map your organization structure to your enrollment hierarchy. For Standard Organization with single IT and single IT budget you may implement single department in EA.  Create a new department for IT if business domains have independent IT capabilities.  Restrict and minimize the number of account owners within the enrollment to avoid the proliferation of admin access to subscriptions and associated Azure resources.  If multiple Azure Active Directory (Azure AD) tenants are used, verify that the account owner is associated with the same tenant as where subscriptions for the account are provisioned.  Set up Enterprise Dev/Test and production environments at an EA account level to support holistic isolation.  Assign a budget for each account, and establish an alert associated with the budget. | Enterprise Agreement enrollment and Azure Active Directory tenants  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/enterprise-enrollment-and-azure-ad-tenants  Cloud governance guides  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/govern/guides/ |
|  |  | We are not following any pattern for creating a new department, account, or subscription in Azure, as part of the cloud adoption strategy. |  |  |  |
|  |  | We are partially using a pattern based on our organizational structure. |  |  |  |
|  |  | We have a well-defined strategy for EA structure and expansion part of our cloud strategy plan. |  |  |  |
| **EA07** | Do you have separation from production and non-production environments at Account level? |  | Enterprise Agreement customers now have a great way to run their development and testing workloads on Azure, with numerous advantages:  Ideal for teams, multiple subscriptions allowed  Access to Dev/Test images in the Gallery, including Windows 8.1 and Windows 10  Special lower Dev/Test rates on Windows Virtual Machines, Cloud Services, SQL Database, HDInsight, App Service and Logic Apps  Additional savings with Reservations for one-year or three-year commitment on VMs and Azure SQL Database  Same great EA rates on other Azure services  Centralized management via the Azure Enterprise Portal  No separate payment—just use the funds already on your Enterprise Agreement  Enterprise Agreement customers have one or more people in the role of Enterprise Administrator, who can access the Azure Enterprise Portal. Enterprise Administrators add users called Account Owners to their agreement via the Azure Enterprise Portal. These Account Owners have the ability to create Azure subscriptions under the EA. The Enterprise Admin needs to check a box under the “Dev/Test” column for an Account Owner so that they have the ability to create Azure subscriptions based on the Enterprise Dev/Test offer. The Account Owner creates subscriptions via the Azure Account Portal, and then should add active Visual Studio subscribers as co-administrators so that they can manage and use the resources needed for development and testing. | Set up Enterprise Dev/Test and production environments at an EA account level to support holistic isolation.  If dev/test and production are going to be isolated environments from an identity perspective, separate them at a tenant level via multiple tenants. | Enterprise Dev/Test  https://azure.microsoft.com/en-us/offers/ms-azr-0148p/  Enterprise Agreement enrollment and Azure Active Directory tenants  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/enterprise-enrollment-and-azure-ad-tenants |
|  |  | No |  |  |  |
|  |  | Most of the environments have a separate account but we have some environments not following this practice. |  |  |  |
|  |  | We have setup Enterprise Dev/Test/production environments at an EA account level to support holistic isolation. |  |  |  |
| **AD01** | What is the strategy around Azure AD tenant(s) with Azure subscriptions and resources? |  | An Azure AD tenant provides identity and access management, which is an important part of your security posture. An Azure AD tenant ensures that authenticated and authorized users have access to only the resources for which they have access permissions. Azure AD provides these services to applications and services deployed in Azure and also to services and applications deployed outside of Azure (such as on-premises or third-party cloud providers).  Azure AD is also used by software as a service applications such as Microsoft 365 and Azure Marketplace. Organizations already using on-premises Active Directory can use their existing infrastructure and extend authentication to the cloud by integrating with Azure AD. Each Azure AD directory has one or more domains. A directory can have many subscriptions associated with it but only one Azure AD tenant.  Ask basic security questions during the Azure AD design phase, such as how your organization manages credentials and how it controls human, application, and programmatic access.  Multiple Azure AD tenants can function in the same enrollment. | Use Azure AD seamless single sign-on based on the selected planning topology.  Multifactor authentication provides another layer of security and a second barrier of authentication. Enforce multifactor authentication and conditional access policies for all privileged accounts for greater security.  Plan and implement for emergency access or break-glass accounts to prevent tenant-wide account lockout.  Use Azure AD Privileged Identity Management for identity and access management.  If dev/test and production are going to be isolated environments from an identity perspective, separate them at a tenant level via multiple tenants.  Avoid creating a new Azure AD tenant unless there's a strong identity and access management justification and processes are already in place. | Enterprise Agreement enrollment and Azure Active Directory tenants  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/enterprise-enrollment-and-azure-ad-tenants  Associate or add an Azure subscription to your Azure Active Directory tenant  https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-how-subscriptions-associated-directory |
|  |  | Some admins created new Azure AD tenants and some subscriptions are managed under those tenants. We do not have a defined a strategy around our Azure AD tenants and subscriptions association and access management and monitoring for Azure resources. |  |  |  |
|  |  | We are using some Azure AD tenants. Azure AD tenants and access to Azure resources are monitored but we do not have a strong identity and access management justification and processes for such structure. |  |  |  |
|  |  | We have a single Azure AD tenant for all subscriptions or we have put in place a policy to provide strong identity and access management justification and processes for managing Azure AD tenants and Azure resources through multiple AAD tenants. |  |  |  |
| **AD02** | What procedures are in place to avoid tenant level lockout? |  | It is important that you prevent being accidentally locked out of your Azure Active Directory (Azure AD) organization because you can't sign in or activate another user's account as an administrator. You can mitigate the impact of accidental lack of administrative access by creating two or more emergency access accounts in your organization.  Emergency access accounts are highly privileged, and they are not assigned to specific individuals. Emergency access accounts are limited to emergency or ""break glass""' scenarios where normal administrative accounts can't be used. We recommend that you maintain a goal of restricting emergency account use to only the times when it is necessary. | Plan and implement for emergency access or break-glass accounts to prevent tenant-wide account lockout:  Accounts should be created as cloud users (no dependency on ADFS or other identity providers)  Break-glass users must not have MFA enabled / enforced.  Break-glass users must be excluded from all Conditional Access Policies.  Break-glass accounts must be member of Global Administrator role in the Azure AD tenant. If PIM used, Break-glass users must remain as permanent members.  Assign strong password to Break-glass accounts.  These accounts should not be used unless there is an emergency. Enable Azure AD logging, so you can monitor sign-in and audit log activity from the emergency accounts and trigger notifications to another administrator.  Document break-glass procedure. | Manage emergency access accounts in Azure AD  https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-emergency-access  Enterprise Agreement enrollment and Azure Active Directory tenants  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/enterprise-enrollment-and-azure-ad-tenants |
|  |  | We do not have break glass accounts configured |  |  |  |
|  |  | We have 1 break glass account configured with/without notifications configured for any activity carried out with the break glass accounts |  |  |  |
|  |  | We have two break glass accounts configured with notifications configured for any activity carried out with the break glass accounts. |  |  |  |

1. Identity and Access Management
   1. Assessment details

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Label | Question | Answer | Why consider this | Suggested Actions | Learn More |
| **IAM01** | Do you currently have a corporate Azure AD tenant? |  | Identity is the new control plane of IT security, so authentication is an organization’s access guard to the new cloud world. Organizations need an identity control plane that strengthens their security and keeps their cloud apps safe from intruders.  An Azure AD tenant provides identity and access management, which is an important part of your security posture. An Azure AD tenant ensures that authenticated and authorized users have access to only the resources for which they have access permissions. Azure AD provides these services to applications and services deployed in Azure and also to services and applications deployed outside of Azure (such as on-premises or third-party cloud providers).  Azure AD is also used by software as a service applications such as Microsoft 365 and Azure Marketplace. Organizations already using on-premises Active Directory can use their existing infrastructure and extend authentication to the cloud by integrating with Azure AD. Each Azure AD directory has one or more domains. A directory can have many subscriptions associated with it but only one Azure AD tenant. | Leverage Azure AD SSO based on the selected planning topology. | Choose the right authentication method for your Azure Active Directory hybrid identity solution  https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn    Enterprise Agreement enrollment and Azure Active Directory tenants  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/enterprise-enrollment-and-azure-ad-tenants |
|  |  | We do not have an Azure AD tenant yet. |  |  |  |
|  |  | We have an Azure AD tenant, and we have users in Azure AD, however the identities are not synced from on-prem AD to Azure AD. |  |  |  |
|  |  | We have a well-defined hybrid identity solution in placed in Azure. |  |  |  |
| **IAM02** | What is the approach to Secure and strengthen user’s authentication process, especially for privileged users? |  | People are connecting to organizational resources in increasingly complicated scenarios. People connect from organization-owned, personal, and public devices on and off the corporate network using smart phones, tablets, PCs, and laptops, often on multiple platforms. In this always-connected, multi-device and multi-platform world, the security of user accounts is more important than ever. Passwords, no matter their complexity, used across devices, networks, and platforms are no longer sufficient to ensure the security of the user account, especially when users tend to reuse passwords across accounts. Sophisticated phishing and other social engineering attacks can result in usernames and passwords being posted and sold across the dark web.  Azure Multi-Factor Authentication (MFA) helps safeguard access to data and applications. It provides an additional layer of security using a second form of authentication. Organizations can use Conditional Access to make the solution fit their specific needs. | Turn on MFA using Conditional Access policies for all users in your organization.  Your MFA rollout plan should include a pilot deployment followed by deployment waves that are within your support capacity. Begin your rollout by applying your Conditional Access policies to a small group of pilot users. After evaluating the effect on the pilot users, process used, and registration behaviors, you can either add more groups to the policy or add more users to the existing groups. | Plan an Azure Multi-Factor Authentication deployment  https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted    Conditional Access: Require MFA for administrators  https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-admin-mfa    Conditional Access: Require MFA for Azure management  https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-azure-management  Conditional Access: Require MFA for all users  https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-all-users-mfa |
|  |  | We do not use MFA. We do not have Azure AD Premium. |  |  |  |
|  |  | We have an Azure AD tenant, and we have users in Azure AD. We use MFA only for a subset of users. |  |  |  |
|  |  | We have AAD Premium and have enabled MFA to all users. We have implemented Conditional Access polices to secure applications and identities. |  |  |  |
| **IAM03** | Are you using Role-based Access Control in Azure for management and data-plane? |  | Using Azure RBAC, you can segregate duties within your team and grant only the amount of access to users that they need to perform their jobs. Instead of giving everybody unrestricted permissions in your Azure subscription or resources, you can allow only certain actions at a particular scope.  When planning your access control strategy, it's a best practice to grant users the least privilege to get their work done. | Use Azure RBAC to manage control and data plane access to resources where possible (e.g., Key Vault, Storage account, Azure SQL Database).  Apply RBAC to Azure AD groups. Add on-premises groups to the "Azure AD only" group if there is an existing group management system already in place.  Use Azure AD Privileged Identity Management (PIM) to establish zero standing access and least privilege. Map your organization's roles to the minimum level of access needed. Azure AD PIM can either be an extension of existing tools and processes, use Azure native tools as outlined, or use both as needed.  Use Azure Security Center just-in-time access for all infrastructure as a service (IaaS) resources to enable network-level protection for ephemeral user access to IaaS virtual machines.  Use Azure-AD-managed identities for Azure resources to avoid authentication based on usernames and passwords. Because many security breaches of public cloud resources originate with credential theft embedded in code or other text sources, enforcing managed identities for programmatic access greatly reduces the risk of credential theft.  Use privileged identities for automation runbooks that require elevated access permissions. Automated workflows that violate critical security boundaries should be governed by the same tools and policies users of equivalent privilege are.  Don't add users directly to Azure resource scopes. This lack of centralized management greatly increases the management required to prevent unauthorized access to restricted data. | Best practices for Azure RBAC  https://docs.microsoft.com/en-us/azure/role-based-access-control/best-practices  Use custom RBAC role definitions within the Azure AD tenant, considering the following key roles  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/identity-and-access-management |
|  |  | We are using few RBAC roles. Not all roles and tasks are mapped into RBAC in Azure yet. |  |  |  |
|  |  | We use RBAC only for managing Azure resources. We have a clear definition of roles and tasks and mapped them to Azure RBAC roles. |  |  |  |
|  |  | We vastly use RBAC for managing Azure resources and use RBAC for data-plane access to resources where possible (e.g., access to secrets inside Azure Key Vault, access to data inside a Storage account, or a SQL Database). |  |  |  |
| **IAM04** | Is Azure RBAC modeled to match Azure Active Directory AAD responsibilities to segregate duties within your teams and grant only the amount of access to users that they need to perform their jobs? |  | Using Azure RBAC, you can segregate duties within your team and grant only the amount of access to users that they need to perform their jobs. Instead of giving everybody unrestricted permissions in your Azure subscription or resources, you can allow only certain actions at a particular scope.  When planning your access control strategy, it's a best practice to grant users the least privilege to get their work done.  IT staff members might feel anxious about their roles and positions as they realize a different set of skills is needed to support cloud solutions. Agile employees who explore and learn new cloud technologies don't need to have that fear. They can lead the adoption of cloud services by helping the organization understand and embrace the associated changes.  The Cloud Adoption Framework guides readers through the full adoption lifecycle. Throughout this framework, readers are provided opportunities to build necessary skills. To help you get started on this journey, skills-readiness articles are included in the following outline for easier access. Each of the following links’ map to the skills required to be successful in each of those adoption phases.  Strategy: Develop the skills needed to prepare an actionable migration plan. This includes business justification and other required business-planning skills.  Plan: Develop the skills needed to prepare an actionable migration plan. This includes business justification and other required business-planning skills.  Ready: Develop the skills needed to prepare the business, culture, people, and environment for coming changes.  Adopt: Adoption skills are aligned to various technical efforts:  Migrate: Gain the skills required to implement the cloud migration plan.  Innovate: Gain the skills needed to deliver innovative new solutions.  Operate: Skills related to the operating model for cloud adoption are aligned to various opportunities to gain skills:  Govern: Gain the skills needed to govern the cloud environment.  Manage: Gain the skills needed to manage a cloud environment.  Monitor: Gain the skills needed to monitor a cloud environment. | Map your organization's roles to the minimum level of access needed.  Use Azure AD Privileged Identity Management (PIM) for Azure and Azure AD roles to establish zero standing access and least privilege.  Azure AD PIM can either be an extension of existing tools and processes, use Azure native tools as outlined, or use both as needed.  **Recommended engagement: Modern Service Management Operational Roles and Tasks for Azure** | Best practices for Azure RBAC  https://docs.microsoft.com/en-us/azure/role-based-access-control/best-practices  Use custom RBAC role definitions within the Azure AD tenant, considering the following key roles  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/identity-and-access-management  Get started on a skills readiness path  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/plan/suggested-skills |
|  |  | We are using few RBAC roles. We are not sure if the assigned roles are aligned \with the organization Identity and Access Management strategy. |  |  |  |
|  |  | We are actively defining and using RBAC roles, but additional design is required to clearly define centralized and delegated responsibilities |  |  |  |
|  |  | We have a mature RBAC implementation fully aligned with the overall organizational Identity & Access Management strategy, with well-defined user access permissions and scopes, aligned with Azure Active Directory users and groups permissions, and combined with Privileged Identity Management capabilities to lower thread exposure times and increase visibility into their use through reports and alerts |  |  |  |
| **IAM05** | What mechanisms or tools are in use to manage, control and monitor access to cloud resources in the organization? |  | Access to privileged Azure resource roles for employees changes over time. To reduce the risk associated with stale role assignments, you should regularly review access. You can use Azure Active Directory (Azure AD) Privileged Identity Management (PIM) to create access reviews for privileged Azure resource roles. You can also configure recurring access reviews that occur automatically. | Use Azure AD RBAC to manage control-plane and data-plane access to resources, where possible. Examples are Azure Key Vault, a storage account, or a SQL database.  Use Azure AD Privileged Identity Management (PIM) for Azure and Azure AD roles to establish zero standing access and least privilege. Map your organization's roles to the minimum level of access needed. Azure AD PIM can either be an extension of existing tools and processes, use Azure native tools as outlined, or use both as needed.  Use Azure AD PIM access reviews to periodically validate resource entitlements. Access reviews are part of many compliance frameworks. As a result, many organizations will already have a process in place to address this requirement.  Integrate Azure AD logs with the platform-central Azure Monitor. Azure Monitor allows for a single source of truth around log and monitoring data in Azure, which gives organizations cloud-native options to meet requirements around log collection and retention.  If any data sovereignty requirements exist, custom user policies can be deployed to enforce them. | What is Azure AD Privileged Identity Management?  https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure  Identity and access management  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/identity-and-access-management |
|  |  | We do not use PIM. (Azure AD Privileged Identity Management) |  |  |  |
|  |  | We use PIM for some Azure AD/Azure roles, but we do not leverage the full potential of the solution across all the different Cloud Services. |  |  |  |
|  |  | We have a mature PIM implementation across several Cloud services, enabling security capabilities such as Just-In-Time Privileged Access, MFA enforcement, auditing and logging or the customer is not licensed for PIM |  |  |  |
| **IAM06** | What is the existing Identity Lifecycle Management solution? |  | Identity Governance helps organizations achieve a balance between productivity - How quickly can a person have access to the resources they need, such as when they join my organization? And security - How should their access change over time, such as due to changes to that person's employment status? Identity lifecycle management is the foundation for Identity Governance, and effective governance at scale requires modernizing the identity lifecycle management infrastructure for applications.  Identity lifecycle  For many organizations, identity lifecycle for employees is tied to the representation of that user in an HCM (human capital management) system. Azure AD Premium automatically maintains user identities for people represented in Workday in both Active Directory and Azure Active Directory, as described in the Workday inbound provisioning tutorial. Azure AD Premium also includes Microsoft Identity Manager, which can import records from on-premises HCM systems such as SAP, Oracle eBusiness, and Oracle PeopleSoft.  Increasingly, scenarios require collaboration with people outside your organization. Azure AD B2B collaboration enables you to securely share your organization's applications and services with guest users and external partners from any organization, while maintaining control over your own corporate data. Azure AD entitlement management enables you to select which organization's users are allowed to request access and be added as B2B guests to your organization's directory and ensures that these guests are removed when they no longer need access. | Use Azure AD RBAC to manage control and data-plane access to resources, where possible. Examples are Azure Key Vault, a storage account, or a SQL database.  Deploy Azure AD conditional-access policies for any user with rights to Azure environments. Doing so provides another mechanism to help protect a controlled Azure environment from unauthorized access.  Enforce multi-factor authentication (MFA) for any user with rights to the Azure environments. MFA enforcement is a requirement of many compliance frameworks. It greatly lowers the risk of credential theft and unauthorized access.  Use Azure AD Privileged Identity Management (PIM) to establish zero standing access and least privilege. Map your organization's roles to the minimum level of access needed. Azure AD PIM can either be an extension of existing tools and processes, use Azure native tools as outlined, or use both as needed.  Use Azure AD-only groups for Azure control-plane resources in Azure AD PIM when you grant access to resources.  Add on-premises groups to the Azure-AD-only group if a group management system is already in place.  Use Azure AD PIM access reviews to periodically validate resource entitlements. Access reviews are part of many compliance frameworks. As a result, many organizations will already have a process in place to address this requirement.  Integrate Azure AD logs with the platform-central Azure Monitor. Azure Monitor allows for a single source of truth around log and monitoring data in Azure, which gives organizations cloud-native options to meet requirements around log collection and retention.  If any data sovereignty requirements exist, custom user policies can be deployed to enforce them. | Azure Active Directory Identity Governance documentation  https://docs.microsoft.com/en-us/azure/active-directory/governance/  Identity and access management  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/identity-and-access-management |
|  |  | We use different solutions to manage identities from On-Prem and the Cloud. These solutions are disconnected duplicating a lot of operation and management tasks. |  |  |  |
|  |  | We have an identity lifecycle management solution that is partially integrated with Azure. We use access reviews for some scenarios. We have a 3rd party solution to manage identity life cycle end to end. This solution is compatible with Azure AD and Active Directory. |  |  |  |
|  |  | We use Azure AD governance capabilities such as PIM, Access Reviews, Entitlement Management etc. Access reviews are part of our compliance frameworks. |  |  |  |
| **IAM07** | What is the current solution in use for monitoring and alerting Azure AD logs in the organization? |  | Azure Monitor allows for a single source of truth around log and monitoring data in Azure, giving organizations a cloud native options to meet requirements around log collection and retention. | Integrate Azure AD logs with the platform-central Azure Monitor. Azure Monitor allows for a single source of truth around log and monitoring data in Azure, which gives organizations cloud-native options to meet requirements around log collection and retention.  Enable Alert Rules related to Azure AD Audit or Sign-in logs, for important events such when there is a sign in related to any break glass account. | Integrate Azure AD logs with Azure Monitor logs  https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-integrate-activity-logs-with-log-analytics  Install and use the log analytics views for Azure Active Directory  https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-install-use-log-analytics-views |
|  |  | We only generate alerts for On-Premises environments. We do not have any monitoring and alerting set up for Azure AD logs. |  |  |  |
|  |  | We use a centralized Cloud Native monitoring solution to monitor and alert for Azure AD logs, but we do not have any alerts configured. |  |  |  |
|  |  | We use Azure Monitor (with/without Azure Sentinel) to monitor and alert for Azure AD logs and we have configured alerts. |  |  |  |
| **IAM08** | What is your current strategy around group membership for privileged accounts in Azure AD related to Identity and Access management? |  | Azure Active Directory (Azure AD) is introducing a public preview in which you can assign a cloud group to Azure AD built-in roles. With this feature, you can use groups to grant admin access in Azure AD with minimal effort from your Global and Privileged role admins.  Consider this example: Contoso has hired people across geographies to manage and reset passwords for employees in its Azure AD organization. Instead of asking a Privileged role admin or Global admin to assign the Helpdesk admin role to each person individually, they can create a ContosoHelpdeskAdministrators group and assign it to the role. When people join the group, they are assigned the role indirectly. Your existing governance workflow can then take care of the approval process and auditing of the group’s membership to ensure that only legitimate users are members of the group and are thus assigned to the Helpdesk admin role. | Use Azure AD-only groups for Azure control-plane resources in Azure AD PIM when you grant access to resources.  Add on-premises groups to the Azure-AD-only group if a group management system is already in place. | Use cloud groups to manage role assignments in Azure Active Directory  https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/roles-groups-concept  Identity and access management  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/identity-and-access-management |
|  |  | We do not use PIM. We assign RBAC roles to users over Azure resources. |  |  |  |
|  |  | We sync our on-premises users and groups to Azure AD and assign Azure RBAC to synced groups. |  |  |  |
|  |  | We use "Azure AD only" groups for Azure control plane resources in Azure AD PIM when granting access to resources. We add on-premises groups to the "Azure AD only" group. |  |  |  |
| **IAM09** | How do you manage the credentials in the code/service principals for authenticating to Azure services? |  | A common challenge when building cloud applications is how to manage the credentials in your code for authenticating to cloud services. Keeping the credentials secure is an important task. Ideally, the credentials never appear on developer workstations and aren't checked into source control. Azure Key Vault provides a way to securely store credentials, secrets, and other keys, but your code has to authenticate to Key Vault to retrieve them.  The managed identities for Azure resources feature in Azure Active Directory (Azure AD) solves this problem. The feature provides Azure services with an automatically managed identity in Azure AD. You can use the identity to authenticate to any service that supports Azure AD authentication, including Key Vault, without any credentials in your code." | Use Azure-AD-managed identities for Azure resources to avoid authentication based on usernames and passwords. Because many security breaches of public cloud resources originate with credential theft embedded in code or other text sources, enforcing managed identities for programmatic access greatly reduces the risk of credential theft | Identity and access management  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/identity-and-access-management  What are managed identities for Azure resources?  https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/ |
|  |  | *We do not have any strategy in place for managing credentials required by the code or the code contains the credentials.* |  |  |  |
|  |  | We have implemented managed identity for few scenarios (e.g., key management in Azure) but it is not clear what is the best option for the short- and long-term goals |  |  |  |
|  |  | We have a well-defined strategy with a well-defined scenario based on their current and future requirements. |  |  |  |
| **IAM10** | Do you have a strategy in place to handle authentication inside a landing zone? |  | A critical design decision that an enterprise organization must make when adopting Azure is whether to extend an existing on-premises identity domain into Azure or to create a brand new one. Requirements for authentication inside the landing zone should be thoroughly assessed and incorporated into plans to deploy Active Directory Domain Services (AD DS) in Windows server, Azure AD Domain Services (Azure AD DS), or both. Most Azure environments will use at least Azure AD for Azure fabric authentication and AD DS local host authentication and group policy management. | Consider centralized and delegated responsibilities to manage resources deployed inside the landing zone.  Applications that rely on domain services and use older protocols can use Azure AD DS.  Use centralized and delegated responsibilities to manage resources deployed inside the landing zone based on role and security requirements.  Privileged operations such as creating service principal objects, registering applications in Azure AD, and procuring and handling certificates or wildcard certificates require special permissions. Consider which users will be handling such requests and how to secure and monitor their accounts with the degree of diligence required.  If an organization has a scenario where an application that uses integrated Windows authentication must be accessed remotely through Azure AD, consider using Azure AD Application Proxy.  There's a difference between Azure AD, Azure AD DS, and AD DS running on Windows server. Evaluate your application needs and understand and document the authentication provider that each one will be using. Plan accordingly for all applications.  Evaluate the compatibility of workloads for AD DS on Windows server and for Azure AD DS.  Ensure your network design allows resources that require AD DS on Windows server for local authentication and management to access the appropriate domain controllers.  For AD DS on Windows server, consider shared services environments that offer local authentication and host management in a larger enterprise-wide network context.  Deploy Azure AD DS within the primary region because this service can only be projected into one subscription.  Use managed identities instead of service principals for authentication to Azure services. This approach reduces exposure to credential theft. | Identity and access management  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/identity-and-access-management |
|  |  | We have an Azure AD Domain Services configured / Active Directory Domain Services (AD DS)in our shared environment. |  |  |  |
|  |  | We are using Azure AD DS / Active Directory Domain Services (AD DS) in Windows server for authentication inside our landing zones. |  |  |  |
|  |  | We have a well-defined strategy around centralized and delegated responsibilities to manage resources deployed inside the landing zone. We use both centralized and delegated responsibilities to manage resources deployed inside the landing zone based on role and security requirements. |  |  |  |

* 1. Additional findings and Recommendations

1. Management Group and Subscription Organization
   1. Assessment details

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Label | Question | Answer | Why consider this | Suggested Actions | Learn More |
| **MG01** | What is the current structure of Management Group in your Azure environment? |  | Management group structures within an Azure Active Directory (Azure AD) tenant support organizational mapping and must be considered thoroughly when an organization plans Azure adoption at scale.  If your organization has many subscriptions, you may need a way to efficiently manage access, policies, and compliance for those subscriptions. Azure management groups provide a level of scope above subscriptions. You organize subscriptions into containers called ""management groups"" and apply your governance conditions to the management groups. All subscriptions within a management group automatically inherit the conditions applied to the management group. Management groups give you enterprise-grade management at a large scale no matter what type of subscriptions you might have. All subscriptions within a single management group must trust the same Azure Active Directory tenant.  For example, you can apply policies to a management group that limits the regions available for virtual machine (VM) creation. This policy would be applied to all management groups, subscriptions, and resources under that management group by only allowing VMs to be created in that region. | Group subscriptions together under management groups aligned within the management group structure and policy requirements at scale. Grouping ensures that subscriptions with the same set of policies and RBAC assignments can inherit them from a management group, which avoids duplicate assignments.  Keep the management group hierarchy reasonably flat with no more than three to four levels, ideally. This restriction reduces management overhead and complexity.  Avoid duplicating your organizational structure into a deeply nested management group hierarchy. Management groups should be used for policy assignment versus billing purposes. This approach necessitates using management groups for their intended purpose in enterprise-scale architecture, which is providing Azure policies for workloads that require the same type of security and compliance under the same management group level.  Create management groups under your root-level management group to represent the types of workloads (archetype) that you'll host, and ones based on their security, compliance, connectivity, and feature needs. This grouping structure allows you to have a set of Azure policies applied at the management group level for all workloads that require the same security, compliance, connectivity, and feature settings.  Create a top-level sandbox management group to allow users to immediately experiment with Azure. Users can then experiment with resources that might not yet be allowed in production environments. The sandbox provides isolation from your development, test, and production environments | Standard enterprise governance guide  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/govern/guides/standard/  Governance guide for complex enterprises  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/govern/guides/complex/  Governance guide for complex enterprises: Multiple layers of governance  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/govern/guides/complex/multiple-layers-of-governance  Management group and subscription organization  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/management-group-and-subscription-organization |
|  |  | We have created a prod and non-prod Management group structure under root. We may have some subscriptions directly under root. |  |  |  |
|  |  | few RBAC and handful policies are assigned at each Management Group. We use a manual process to assign RBAC and Azure Policy. We move subscriptions from root under their corresponding Management Groups. |  |  |  |
|  |  | We have created our management groups structure under root-level management group to represent the types of workloads (archetype) that we host, and ones based on our security, compliance, connectivity, and feature needs. This allows allow us to have a set of Azure policies applied at the management group level for all workloads that require the same security, compliance, connectivity, and feature settings. No subscriptions stay directly below root. |  |  |  |
| **MG02** | Below root how many levels of Management Groups you have? |  | A management group tree can support up to six levels of depth. This limit doesn't include the tenant root level or the subscription level. | Keep the management group hierarchy reasonably flat with no more than three to four levels, ideally. This restriction reduces management overhead and complexity.  Avoid duplicating your organizational structure into a deeply nested management group hierarchy. Management groups should be used for policy assignment versus billing purposes. This approach necessitates using management groups for their intended purpose in enterprise-scale architecture, which is providing Azure policies for workloads that require the same type of security and compliance under the same management group level.  Create management groups under your root-level management group to represent the types of workloads (archetype) that you'll host, and ones based on their security, compliance, connectivity, and feature needs. This grouping structure allows you to have a set of Azure policies applied at the management group level for all workloads that require the same security, compliance, connectivity, and feature settings. | What are Azure management groups?  https://docs.microsoft.com/en-us/azure/governance/management-groups/overview  Management group and subscription organization  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/management-group-and-subscription-organization |
|  |  | 0 or 1 |  |  |  |
|  |  | more than 4 |  |  |  |
|  |  | 2 to 4 |  |  |  |
| **MG03** | Do you use Azure tags to query and horizontally navigate across the Management Group hierarchy? |  | Using tags allows you to have a chargeback mechanism for workloads that share a subscription or for a given workload that spans across multiple subscriptions. | Use Azure resource tags for cost categorization and resource grouping.  When you apply metadata tags to your cloud resources, you can include information about those assets that couldn't be included in the resource name. You can use that information to perform more sophisticated filtering and reporting on resources. You want these tags to include context about the resource's associated workload or application, operational requirements, and ownership information. This information can be used by IT or business teams to find resources or generate reports about resource usage and billing.  What tags you apply to resources and what tags are required or optional differs among organizations.  Use resource tags, which can be enforced or appended through Azure Policy, to query and horizontally navigate across the management group hierarchy. Then you can group resources for search needs without having to use a complex management group hierarchy. | Recommended naming and tagging conventions  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/naming-and-tagging  Management group and subscription organization  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/management-group-and-subscription-organization  Manage tag governance with Azure Policy  https://docs.microsoft.com/en-us/azure/governance/policy/tutorials/govern-tags |
|  |  | We apply tags to Azure resources manually or using scripting. |  |  |  |
|  |  | We apply tags to Azure resources using Policy but in general tags are not consistent across Azure resources in our environment. |  |  |  |
|  |  | We apply tags through Azure Policy, to query and horizontally navigate across the management group hierarchy. This facilitates grouping resources for search needs without having to use a complex management group hierarchy |  |  |  |
| **MG04** | How do you manage Management Groups? |  | Using a Service Principal reduces the number of users who have elevated rights and follows least-privilege guidelines. | Use a dedicated service principal name (SPN) to execute management group management operations, subscription management operations, and role assignment. Using an SPN reduces the number of users who have elevated rights and follows least-privilege guidelines.  Assign the User Access Administrator Azure role-based access control (RBAC) role at the root management group scope (/) to grant the SPN just mentioned access at the root level. After the SPN is granted permissions, the User Access Administrator role can be safely removed. In this way, only the SPN is part of the User Access Administrator role.  Assign Contributor permission to the SPN previously mentioned at the root management group scope (/), which allows tenant-level operations. This permission level ensures that the SPN can be used to deploy and manage resources to any subscription within your organization.  Limit the number of Azure Policy assignments made at the root management group scope (/). This limitation minimizes debugging inherited policies in lower-level management groups.  Don't create any subscriptions under the root management group. This hierarchy ensures that subscriptions don't only inherit the small set of Azure policies assigned at the root-level management group, which don't represent a full set necessary for a workload. | Management group and subscription organization  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/management-group-and-subscription-organization |
|  |  | We manage Azure Management Groups using Owner role assigned to our administrators. |  |  |  |
|  |  | We manage Azure Management Groups using User Access Administrator role assigned to our administrators. |  |  |  |
|  |  | We use a dedicated service principal (SPN) to execute management group management operations, subscription management operations, and role assignment. We assign the User Access Administrator RBAC role at the tenant root scope (/) to grant the SPN mentioned above access at the root level. |  |  |  |
| **MG05** | Do you have a dedicated Management Group structure for platform resources? |  | Create a Platform management group under the root management group to support common platform policy and RBAC assignment. This grouping structure ensures that different policies can be applied to the subscriptions used for your Azure foundation. It also ensures that the billing for common resources is centralized in one set of foundational subscriptions. | Establish a dedicated management subscription in the Platform management group to support global management capabilities such as Azure Monitor Log Analytics workspaces and Azure Automation runbooks.  Establish a dedicated identity subscription in the Platform management group to host Windows server Active Directory domain controllers, when necessary.  Establish a dedicated connectivity subscription in the Platform management group to host an Azure Virtual WAN hub, private Domain Name System (DNS), ExpressRoute circuit, and other networking resources. A dedicated subscription ensures that all foundation network resources are billed together and isolated from other workloads. | Management group and subscription organization  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/management-group-and-subscription-organization |
|  |  | We keep platform related Azure resources under root management group inside "production" management group in the same subscription as production workloads. |  |  |  |
|  |  | We keep platform related Azure resources under root management group inside "production" management group in separate subscription(s) as production workloads. |  |  |  |
|  |  | We have a Platform Management Group under our top-level Management Group to support common platform policy and RBAC assignment. |  |  |  |
| **SU01** | Is there a dedicated management subscription to support global management capabilities? |  | Establish a dedicated management subscription in the Platform management group to support global management capabilities such as Azure Monitor Log Analytics workspaces and Azure Automation runbooks. | Establish a dedicated management subscription in the Platform management group to support global management capabilities such as Azure Monitor Log Analytics workspaces and Azure Automation runbooks. | Management group and subscription organization  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/management-group-and-subscription-organization |
|  |  | All management resources are in production or non-production subscriptions. |  |  |  |
|  |  | We have a dedicated subscription for all connectivity, identity, and management group resources. |  |  |  |
|  |  | We have established a dedicated management subscription in the Platform management group to support global management capabilities such as Azure Monitor Log Analytics workspaces and Azure Automation runbooks. |  |  |  |
| **SU02** | Is there a dedicated subscription for hosting Windows Server Active Directory domain controllers? |  | Establish a dedicated identity subscription in the Platform management group to host Windows server Active Directory domain controllers, when necessary. | Establish a dedicated identity subscription in the Platform management group to host Windows server Active Directory domain controllers, when necessary. | Management group and subscription organization  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/management-group-and-subscription-organization |
|  |  | All identity related resources are in production or non-production subscriptions. |  |  |  |
|  |  | We have a dedicated subscription for all connectivity, identity, and management group resources. |  |  |  |
|  |  | We have a dedicated identity subscription in the Platform management group to host Windows Server Active Directory domain controllers, when necessary. |  |  |  |
| **SU03** | Is there a dedicated subscription for hosting connectivity resources (Virtual WAN hub, Express Route circuit, etc.)? |  | Establish a dedicated connectivity subscription in the Platform management group to host an Azure Virtual WAN hub, private Domain Name System (DNS), ExpressRoute circuit, and other networking resources. A dedicated subscription ensures that all foundation network resources are billed together and isolated from other workloads. | Establish a dedicated connectivity subscription in the Platform management group to host an Azure Virtual WAN hub, private Domain Name System (DNS), ExpressRoute circuit, and other networking resources. A dedicated subscription ensures that all foundation network resources are billed together and isolated from other workloads. | Management group and subscription organization  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/management-group-and-subscription-organization |
|  |  | All connectivity related resources are in production or non-production subscriptions. |  |  |  |
|  |  | We have a dedicated subscription for all connectivity, identity, and management group resources. |  |  |  |
|  |  | We have established a dedicated connectivity subscription in the Platform management group to host an Azure Virtual WAN hub, private DNS, ExpressRoute circuit, and other networking resources. This ensures that all foundation network resources are billed together and isolated from other workloads. |  |  |  |
| **SU04** | Are Subscription owners performing regular access reviews? |  | With Azure Active Directory (Azure AD), you can easily ensure that users have appropriate access. Access to privileged Azure resource roles for employees changes over time. To reduce the risk associated with stale role assignments, you should regularly review access. You can use Azure Active Directory (Azure AD) Privileged Identity Management (PIM) to create access reviews for privileged Azure resource roles. You can also configure recurring access reviews that occur automatically. | Make subscription owners aware of their roles and responsibilities:  Perform an access review in Azure AD Privileged Identity Management quarterly or twice a year to ensure that privileges don't proliferate as users move within the customer organization.  Take full ownership of budget spending and resource utilization.  Ensure policy compliance and remediate when necessary. | Create an access review of Azure resource roles in Privileged Identity Management  https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-start-access-review  Management group and subscription organization  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/management-group-and-subscription-organization |
|  |  | We assign RBAC and never review the assigned roles. |  |  |  |
|  |  | We review the assigned roles on azure resources frequently through a manual process. We do not have an automated process to perform the access review. |  |  |  |
|  |  | We perform an access review in Azure AD Privileged Identity Management quarterly or twice a year to ensure that privileges don't proliferate as users move within the customer organization. |  |  |  |
| **SU05** | How do you manage subscriptions quotas and optimize consumptions? |  | Azure subscriptions have adjustable limits for some services. For example, the number of virtual networks in a subscription is limited. When a subscription approaches these limits, you'll need to create another subscription and put additional resources there. For more information, see Azure subscription and service limits.  If you want to raise the limit or quota above the default limit, you will be required to open an online customer support request at no charge.  The terms soft limit and hard limit often are used informally to describe the current, adjustable limit (soft limit) and the maximum limit (hard limit). If a limit isn't adjustable, there won't be a soft limit, only a hard limit. | Consider limits and quotas within the Azure platform for each service that your workloads require.  Consider the availability of required SKUs within chosen Azure regions. For example, new features might be available only in certain regions. The availability of certain SKUs for given resources such as VMs might be different from one region to another.  Consider that subscription quotas aren't capacity guarantees and are applied on a per-region basis.  Use subscriptions as scale units and scale out resources and subscriptions as required. Your workload can then use the required resources for scaling out, when needed, without hitting subscription limits in the Azure platform.  Use reserved instances to prioritize reserved capacity in required regions. Then your workload will have the required capacity even when there's a high demand for that resource in a specific region.  Establish a dashboard with custom views to monitor used capacity levels. Set up alerts if capacity utilization is reaching critical levels (for example, 90 percent CPU utilization).  Raise support requests for quota increase as a part of subscription provisioning (for example, total available VM cores within a subscription). This approach ensures your quota limits are set before your workloads require going over the default limits.  Ensure required services and features are available within the chosen deployment regions. | Management group and subscription organization  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/management-group-and-subscription-organization  Azure subscription and service limits, quotas, and constraints  https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/azure-subscription-service-limits    https://docs.microsoft.com/en-us/archive/blogs/tomholl/get-alerts-as-you-approach-your-azure-resource-quotas |
|  |  | We have seen errors related to capability and we open a support ticket to solve the issue when this happens. |  |  |  |
|  |  | We have set up an Alert to report us when an Azure quota is reaching x% of capacity. |  |  |  |
|  |  | We configure quota increase as a part of subscription provisioning (e.g., total available VM cores within a subscription). We have a dashboard with custom views / workbooks to monitor utilized capacity levels. We have set up alerts if capacity utilization is reaching critical levels (e.g., 90% CPU utilization). we use Azure Reservations. |  |  |  |
| **SU06** | Is your subscriptions model following any business, lifecycle, department, or application pattern? Is this pattern aligned with the Management Groups hierarchy? |  | Subscriptions should be used as a unit of management and scale aligned with business needs and priorities to support business areas and portfolio owners to accelerate application migrations and new application development. Subscriptions should be provided to business units to support the design, development, and testing of new workloads and migration of workloads. | Use the following principles when identifying requirements for new subscriptions:  Scale limits: Subscriptions serve as a scale unit for component workloads to scale within platform subscription limits. For example, large, specialized workloads such as high-performance computing, IoT, and SAP are all better suited to use separate subscriptions to avoid limits (such as a limit of 50 Azure Data Factory integrations).  Management boundary: Subscriptions provide a management boundary for governance and isolation, which allows for a clear separation of concerns. For example, different environments such as development, test, and production are often isolated from a management perspective.  Policy boundary: Subscriptions serve as a boundary for the assignment of Azure policies. For example, secure workloads such as PCI typically require additional policies to achieve compliance. This additional overhead doesn't need to be considered holistically if a separate subscription is used. Similarly, development environments might have more relaxed policy requirements relative to production environments.  Target network topology: Virtual networks can't be shared across subscriptions, but they can connect with different technologies such as virtual network peering or Azure ExpressRoute. Consider which workloads must communicate with each other when you decide whether a new subscription is required. | Management group and subscription organization  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/management-group-and-subscription-organization  Create additional subscriptions to scale your Azure environment  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/scale-subscriptions |
|  |  | We create subscriptions as needed. |  |  |  |
|  |  | Functional Pattern (Based on departments, department owners, and department projects)  Geographic Pattern (Based on customer locations, location owners, and location projects)  Business Pattern (Based on business units, business Owners and business projects) |  |  |  |
|  |  | Application Pattern (based on application and environments) |  |  |  |

* 1. Additional findings and Recommendations

1. Network Topology and Connectivity
   1. Assessment details

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Label | Question | Answer | Why consider this | Suggested Actions | Learn More |
| **NET01** | Have you defined your network address spaces for workloads in Azure? |  | Overlapping IP address spaces across on-premises and Azure regions will create major contention challenges.  You can add address space after you create a virtual network. This process requires an outage if the virtual network is already connected to another virtual network via virtual network peering because the peering must be deleted and re-created.  Azure reserves five IP addresses within each subnet. Factor in those addresses when you're sizing virtual networks and encompassed subnets.  Some Azure services require dedicated subnets. These services include Azure Firewall and Azure VPN Gateway.  You can delegate subnets to certain services to create instances of a service within the subnet. | Plan for non-overlapping IP address spaces across Azure regions and on-premises locations well in advance.  Use IP addresses from the address allocation for private internets (RFC 1918).  Don't create unnecessarily large virtual networks (for example, /16) to ensure that IP address space isn't wasted.  Don't create virtual networks without planning the required address space in advance. Adding address space will cause an outage after a virtual network is connected via virtual network peering. | Network topology and connectivity  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/network-topology-and-connectivity  Azure best practices for network security  https://docs.microsoft.com/en-us/azure/security/fundamentals/network-best-practices |
|  |  | We have defined few Azure VNets and address spaces in Azure as needed. |  |  |  |
|  |  | Our networking team provided some non-overlapping address spaces to use in Azure. |  |  |  |
|  |  | Our networking team have defined a structure of non-overlapping address spaces for Azure. We have a clear segmentation for production, non-production workloads as well as internal vs external traffic. |  |  |  |
| **NET02** | What better describes your networking requirements in Azure? |  | Network topology is a critical element of the enterprise-scale architecture because it defines how applications can communicate with each other. This section explores technologies and topology approaches for enterprise Azure deployments. It focuses on two core approaches: topologies based on Azure Virtual WAN, and traditional topologies. | Use Cloud-only Azure network topology if you need to start with Landing Zones for your workloads in Azure, where there is no on-premises network footprint or hybrid connectivity to on-premises datacenter is not required from the start.  Use a Hub and Spoke Azure network topology if any of the following are true:   * Your organization intends to deploy resources in only a few Azure regions. * You don't need a global interconnected network. * You have a low number of remote or branch locations per region. That is, you need fewer than 30 IP security (IPsec) tunnels. * You require full control and granularity for manually configuring your Azure network.   Use a network topology based on Azure Virtual WAN if any of the following are true:   * Your organization intends to deploy resources across several Azure regions and needs to connect your global locations to both Azure and on-premises. * Your organization intends to use software-defined WAN (SD-WAN) deployments fully integrated with Azure. * You intend to deploy up to 2,000 virtual machine workloads across all VNets connected to a single Azure Virtual WAN hub.   We recommend Virtual WAN for new large or global network deployments in Azure where you need global transit connectivity across Azure regions and on-premises locations. That way, you don't have to manually set up transitive routing for Azure networking | Network topology and connectivity  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/network-topology-and-connectivity  Hub-spoke network topology in Azure  https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke  Global transit network architecture and Virtual WAN  https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-global-transit-network-architecture |
|  |  | We only need Azure network without hybrid connectivity |  |  |  |
|  |  | We require on-premises connectivity with Hub and Spoke topology. |  |  |  |
|  |  | We require on-premises connectivity using Azure vWAN, because we have more than 30 branch locations / we are looking for global transitivity / we do not need granular control and configuration on spoke networks. |  |  |  |
| **NET03** | Do you have a dedicated Hub VNet in your Azure environment? |  | Cost savings and scalability by centralizing services that can be shared by multiple workloads, such as network virtual appliances (NVAs).  Overcome subscriptions limits by peering VNets from different subscriptions to the central hub.  Separation of concerns between central IT (SecOps, InfraOps) and workloads (DevOps). | Use a traditional Azure network topology if any of the following are true:  Your organization intends to deploy resources in only a few Azure regions.  You don't need a global interconnected network.  You have a low number of remote or branch locations per region. That is, you need fewer than 30 IP security (IPsec) tunnels.  You require full control and granularity for manually configuring your Azure network.  This traditional topology helps you build a secure network foundation in Azure. | Network topology and connectivity  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/network-topology-and-connectivity  Hub-spoke network topology in Azure  https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke  Global transit network architecture and Virtual WAN  https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-global-transit-network-architecture |
|  |  | We have a Hub Network, but all other VNets are connected to each other through VNet peering as mesh. |  |  |  |
|  |  | We have one or more Hub and Spoke network topology in Azure. there is a firewall in Hub and spokes are connected only to hub. |  |  |  |
|  |  | We have Virtual WAN topology in Azure. |  |  |  |
| **NET04** | What is the hybrid connectivity strategy? |  | The virtual network gateway enables the virtual network to connect to the VPN device, or ExpressRoute circuit, used for connectivity with your on-premises network.  Virtual networks don't traverse subscription boundaries. But you can achieve connectivity between virtual networks in different subscriptions by using virtual network peering, an ExpressRoute circuit, or VPN gateways.  Network Site-to-site A site-to-site VPN allows you to create a secure connection between your on-premises site and your virtual network. We use industry standard IPsec VPN in Azure. So we are interoperable with most VPN devices. You can use this service to connect to 30 on-premises sites and virtual networks to each other securely with aggregated bandwidth between 100 Mbps to max 10 Gbps.  ExpressRoute lets you create private connections between Azure datacenters and infrastructure that’s on your premises or in a co-location environment. ExpressRoute connections do not go over the public Internet, and offer more reliability, faster speeds, lower latencies, and higher security than typical connections over the Internet. With ExpressRoute, you can establish connections to Azure at an ExpressRoute location (Exchange Provider facility) or directly connect to Azure from your existing WAN network (such as a MPLS VPN) provided by a network service provider.  Although the hybrid networking architecture supports VPN connections, dedicated WAN connections like ExpressRoute are preferred due to higher performance and increased security. | Consider a network design based in the hub-and-spoke network topology with non-Virtual WAN technologies for the following scenarios:   * The traffic boundary in an Azure deployment is within an Azure region. * A network architecture has up to two Azure regions, and there's a requirement for transit connectivity between virtual networks for landing zones across regions. * A network architecture spans multiple Azure regions, and there's no need for transitive connectivity between virtual networks for landing zones across regions. * There's no need for transitive connectivity between VPN and ExpressRoute connections. * The main cross-premises connectivity channel is ExpressRoute, and the number of VPN connections is less than 30 per VPN gateway. * There's a heavy dependency on centralized NVAs and complex/granular routing.   For regional deployments, primarily use the hub-and-spoke topology. Use landing-zone virtual networks that connect with virtual network peering to a central-hub virtual network for cross-premises connectivity via ExpressRoute, VPN for branch connectivity, spoke-to-spoke connectivity via NVAs and UDRs, and internet-outbound protection via NVA. The following figure shows this topology. This allows for appropriate traffic control to meet most requirements for segmentation and inspection.  Use the topology of multiple virtual networks connected with multiple ExpressRoute circuits when one of these conditions is true:   * You need a high level of isolation. * You need dedicated ExpressRoute bandwidth for specific business units. * You've reached the maximum number of connections per ExpressRoute gateway (up to four).   Consider alternatives to “force-tunneling” of Internet-outbound traffic, like utilizing the Checkpoint F/W itself (or if exploring even further alternatives, Azure F/W) for internet-outbound  Consider extending Hub-and-Spoke architecture towards a 2-Location (Region) approach, for increased availability and scalability, with dual-ER connections, as per https://docs.microsoft.com/en-us/azure/expressroute/designing-for-disaster-recovery-with-expressroute-privatepeering | Software Defined Networking: Hybrid network  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/decision-guides/software-defined-network/hybrid  What is VPN Gateway?  https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways  What is Azure ExpressRoute?  https://docs.microsoft.com/en-us/azure/expressroute/expressroute-introduction  Network topology and connectivity  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/network-topology-and-connectivity" |
|  |  | We have one or more Site to Site VPN between Azure and our on-premises datacenters |  |  |  |
|  |  | We have one or more ExpressRoute circuits between Azure and our on-premises network. |  |  |  |
|  |  | We have one or more ExpressRoute circuits between Azure and our on-premises network in a Virtual WAN topology. |  |  |  |
| **NET05** | What is your name resolution strategy in Azure? |  | Domain Name System (DNS) is a critical design topic in the overall enterprise-scale architecture. Some organizations might want to use their existing investments in DNS. Others might see cloud adoption as an opportunity to modernize their internal DNS infrastructure and use native Azure capabilities.  You can use a DNS resolver in conjunction with Azure Private DNS for cross-premises name resolution.  You might require the use of existing DNS solutions across on-premises and Azure.  The maximum number of private DNS zones to which a virtual network can link with auto-registration is one.  The maximum number of private DNS zones to which a virtual network can link is 1,000 without auto-registration enabled. | For environments where name resolution in Azure is all that's required, use Azure Private DNS for resolution. Create a delegated zone for name resolution (such as azure.contoso.com).  For environments where name resolution across Azure and on-premises is required, use existing DNS infrastructure (for example, Active Directory integrated DNS) deployed onto at least two Azure virtual machines (VMs). Configure DNS settings in virtual networks to use those DNS servers.  You can still link an Azure Private DNS zone to the virtual networks and use DNS servers as hybrid resolvers with conditional forwarding to on-premises DNS names, such as onprem.contoso.com, by using on-premises DNS servers. You can configure on-premises servers with conditional forwarders to resolver VMs in Azure for the Azure Private DNS zone (for example, azure.contoso.com).  Special workloads that require and deploy their own DNS (such as Red Hat OpenShift) should use their preferred DNS solution.  Enable auto-registration for Azure DNS to automatically manage the lifecycle of the DNS records for the virtual machines deployed within a virtual network.  Use a virtual machine as a resolver for cross-premises DNS resolution with Azure Private DNS.  Create the Azure Private DNS zone within a global connectivity subscription. You might create other Azure Private DNS zones (for example, privatelink.database.windows.net or privatelink.blob.core.windows.net for Azure Private Link).  Even if DCs were brought in Azure, non-domain authoritative (e.g., Internet) DNS queries for domain-joined VMs, would be directed to the on-premises DNS, to be forwarded from there to internet. This is a consequence of the overall “force-tunneling” approach. Consider simplifying name resolution approach for VM systems that do require AD DNS name resolution (e.g., for domain-joined systems), for example by allowing Route Hints or specific forwarders, onto the Azure DCs, while relaxing full “force-tunneling” through on-premises. | Name resolution for resources in Azure virtual networks  https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-name-resolution-for-vms-and-role-instances  Azure DNS Private zones scenarios  https://docs.microsoft.com/en-us/azure/dns/private-dns-scenarios  Network topology and connectivity  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/network-topology-and-connectivity" |
|  |  | We do not have a clear strategy. In Some VNets we use Azure VNets internal DNS, in some VNets we have a custom DNS. |  |  |  |
|  |  | We have our custom DNS setup for all Azure VNets in Azure to be able to perform name resolutions across all workloads in Azure and on-premises workloads. |  |  |  |
|  |  | We use Azure Private DNS Zones in Azure VNets. |  |  |  |
| **NET06** | How many networking locations do you have or require in Azure as Hub? |  | We recommend Virtual WAN for new large or global network deployments in Azure where you need global transit connectivity across Azure regions and on-premises locations. That way, you don't have to manually set up transitive routing for Azure networking. Virtual WAN greatly simplifies end-to-end network connectivity in Azure and cross-premises by creating a hub-and-spoke network architecture. The architecture spans multiple Azure regions and on-premises locations (any-to-any connectivity) out of the box.  Use traditional Hub and Spoke model If a global transitive network across multiple Azure regions or cross-premises isn't required. An example is a branch in the United States that requires connectivity to a virtual network in Europe.  Use a traditional Azure network topology if you have a low number of remote or branch locations per region. That is, you need fewer than 30 IP security (IPsec) tunnels. | For regional deployments, primarily use the hub-and-spoke topology. Use landing-zone virtual networks that connect with virtual network peering to a central-hub virtual network for cross-premises connectivity via ExpressRoute, VPN for branch connectivity, spoke-to-spoke connectivity via NVAs and UDRs, and internet-outbound protection via NVA. This allows for appropriate traffic control to meet most requirements for segmentation and inspection.  When you deploy a hub-and-spoke network architecture in two Azure regions and transit connectivity between all landing zones across regions is required, use ExpressRoute with dual circuits to provide transit connectivity for landing-zone virtual networks across Azure regions. In this scenario, landing zones can transit within a region via NVA in local-hub virtual network and across regions via ExpressRoute circuit. Traffic must hairpin at the MSEE routers.  When your organization requires hub-and-spoke network architectures across more than two Azure regions and global transit connectivity between landing zones, virtual networks across Azure regions are required. You can implement this architecture by interconnecting central-hub virtual networks with global virtual network peering and using UDRs and NVAs to enable global transit routing. Because the complexity and management overhead are high, we recommend deploying a global transit network architecture with Virtual WAN. | Network topology and connectivity  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/network-topology-and-connectivity |
|  |  | We do not have/need a hub Vnet |  |  |  |
|  |  | One Hub VNet / One Location |  |  |  |
|  |  | Two or more Hub VNets / Two or more locations |  |  |  |
| **NET07** | How do you manage load balancing in the application layer in Azure? |  | Azure Load Balancer (internal and public) provides high availability for app delivery at a regional level.  Azure Application Gateway allows the secure delivery of HTTP/S apps at a regional level.  Azure Front Door Service allows the secure delivery of highly available HTTP/S apps across Azure regions.  Azure Traffic Manager allows the delivery of global apps.  When selecting the load-balancing options, here are some factors to consider:  Traffic type. Is it a web (HTTP/HTTPS) application? Is it public facing or a private application?  Global versus. regional. Do you need to load balance VMs or containers within a virtual network, or load balance scale unit/deployments across regions, or both?  Availability. What is the service SLA?  Cost. See Azure pricing. In addition to the cost of the service itself, consider the operations cost for managing a solution built on that service.  Features and limits. What are the overall limitations of each service? See Service limits. | Availability is a key component of any security program. If your users and systems can't access what they need to access over the network, the service can be considered compromised. Azure has networking technologies that support the following high-availability mechanisms:   * HTTP-based load balancing * Network level load balancing * Global load balancing   Load balancing is a mechanism designed to equally distribute connections among multiple devices. The goals of load balancing are:  To increase availability. When you load balance connections across multiple devices, one or more of the devices can become unavailable without compromising the service. The services running on the remaining online devices can continue to serve the content from the service.  To increase performance. When you load balance connections across multiple devices, a single device doesn't have to handle all processing. Instead, the processing and memory demands for serving the content is spread across multiple devices.  Azure Front Door is an application delivery network that provides global load balancing and site acceleration service for web applications. It offers Layer 7 capabilities for your application like SSL offload, path-based routing, fast failover, caching, etc. to improve performance and high-availability of your applications.  At this time, Azure Front Door does not support Web Sockets.  Traffic Manager is a DNS-based traffic load balancer that enables you to distribute traffic optimally to services across global Azure regions, while providing high availability and responsiveness. Because Traffic Manager is a DNS-based load-balancing service, it load balances only at the domain level. For that reason, it can't fail over as quickly as Front Door, because of common challenges around DNS caching and systems not honoring DNS TTLs.  Application Gateway provides application delivery controller (ADC) as a service, offering various Layer 7 load-balancing capabilities. Use it to optimize web farm productivity by offloading CPU-intensive SSL termination to the gateway.  Azure Load Balancer is a high-performance, low-latency Layer 4 load-balancing service (inbound and outbound) for all UDP and TCP protocols. It is built to handle millions of requests per second while ensuring your solution is highly available. Azure Load Balancer is zone-redundant, ensuring high availability across Availability Zones.  Perform app delivery within landing zones for both internal-facing and external-facing apps.  For secure delivery of HTTP/S apps, use Application Gateway v2 and ensure that WAF protection and policies are enabled.  Use a partner NVA if you can't use Application Gateway v2 for the security of HTTP/S apps.  Deploy Azure Application Gateway v2 or partner NVAs used for inbound HTTP/S connections within the landing-zone virtual network and with the apps that they're securing.  Use a DDoS standard protection plan for all public IP addresses in a landing zone.  Use Azure Front Door Service with WAF policies to deliver and help protect global HTTP/S apps that span Azure regions.  When you're using Azure Front Door Service and Application Gateway to help protect HTTP/S apps, use WAF policies in Azure Front Door Service. Lock down Application Gateway to receive traffic only from Azure Front Door Service.  Use Traffic Manager to deliver global apps that span protocols other than HTTP/S. | Overview of load-balancing options in Azure  https://docs.microsoft.com/en-us/azure/architecture/guide/technology-choices/load-balancing-overview  Network topology and connectivity  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/network-topology-and-connectivity |
|  |  | We use a third-party solution. |  |  |  |
|  |  | We use Azure Application Gateway / Load Balancer. |  |  |  |
|  |  | We use Azure Application Gateway / Load Balancer with Traffic Manager / Front Door for geo redundancy. |  |  |  |
| **NET08** | How do you manage load balancing for TCP traffic in Azure? |  | With Standard Load Balancer, you can scale your applications and create highly available services. Load balancer supports both inbound and outbound scenarios. Load balancer provides low latency and high throughput and scales up to millions of flows for all TCP and UDP applications.  Key scenarios that you can accomplish using Standard Load Balancer include:  Load balance internal and external traffic to Azure virtual machines.  Increase availability by distributing resources within and across zones.  Configure outbound connectivity for Azure virtual machines.  Use health probes to monitor load-balanced resources.  Employ port forwarding to access virtual machines in a virtual network by public IP address and port.  Enable support for load-balancing of IPv6.  Standard Load Balancer provides multi-dimensional metrics through Azure Monitor. These metrics can be filtered, grouped, and broken out for a given dimension. They provide current and historic insights into performance and health of your service. Resource Health is also supported. Review Standard Load Balancer Diagnostics for more details.  Load balance services on multiple ports, multiple IP addresses, or both.  Move internal and external load balancer resources across Azure regions.  Load balance TCP and UDP flow on all ports simultaneously using HA ports. | Use Azure Load Balancer for high-performance, low-latency Layer 4 load-balancing service (inbound and outbound) for all UDP and TCP protocols. Azure Load Balancer is built to handle millions of requests per second while ensuring your solution is highly available. Azure Load Balancer is zone-redundant, ensuring high availability across Availability Zones. | What is Azure Load Balancer?  https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview  Network topology and connectivity  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/network-topology-and-connectivity |
|  |  | We use a third-party solution. |  |  |  |
|  |  | We use Azure Load Balancer. |  |  |  |
|  |  | We use Azure Load Balancer with Traffic Manager for geo redundancy. |  |  |  |
| **NET09** | What is your strategy for zero-trust networking? |  | The zero-trust model assumes a breached state and verifies each request as though it originates from an uncontrolled network.  An advanced zero-trust network implementation employs fully distributed ingress/egress cloud micro-perimeters and deeper micro-segmentation.  Network security groups can use Azure service tags to facilitate connectivity to Azure PaaS services.  App security groups don't span or provide protection across virtual networks.  NSG flow logs are now supported through Azure Resource Manager templates. | Delegate subnet creation to the landing zone owner. This will enable them to define how to segment workloads across subnets (for example, a single large subnet, multitier app, or network-injected app). The platform team can use Azure Policy to ensure that an NSG with specific rules (such as deny inbound SSH or RDP from internet or allow/block traffic across landing zones) is always associated with subnets that have deny-only policies.  Use NSGs to help protect traffic across subnets, as well as east/west traffic across the platform (traffic between landing zones).  If you need basic network level access control (based on IP address and the TCP or UDP protocols), you can use Network Security Groups (NSGs). An NSG is a basic, stateful, packet filtering firewall, and it enables you to control access based on a 5-tuple. NSGs include functionality to simplify management and reduce the chances of configuration mistakes:  Augmented security rules simplify NSG rule definition and allow you to create complex rules rather than having to create multiple simple rules to achieve the same result.  Service tags are Microsoft created labels that represent a group of IP addresses. They update dynamically to include IP ranges that meet the conditions that define inclusion in the label. For example, if you want to create a rule that applies to all Azure storage on the east region you can use Storage.EastUS  Application security groups allow you to deploy resources to application groups and control the access to those resources by creating rules that use those application groups. For example, if you have webservers deployed to the 'Webservers' application group you can create a rule that applies a NSG allowing 443 traffic from the Internet to all systems in the 'Webservers' application group.  NSGs do not provide application layer inspection or authenticated access controls.  The app team should use app security groups at the subnet-level NSGs to help protect multitier VMs within the landing zone.  Use NSGs and app security groups to micro-segment traffic within the landing zone and avoid using a central NVA to filter traffic flows.  Enable NSG flow logs and feed them into Traffic Analytics to gain insights into internal and external traffic flows.  Use NSGs to selectively allow connectivity between landing zones.  Deploy Azure Firewall in Virtual WAN hubs for east/west and south/north traffic protection and filtering within an Azure region.  For Virtual WAN topologies, route traffic across landing zones via Azure Firewall if your organization requires filtering and logging capabilities for traffic flowing across landing zones. | Azure network security overview  https://docs.microsoft.com/en-us/azure/security/fundamentals/network-overview  Network topology and connectivity  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/network-topology-and-connectivity  What is Azure Firewall?  https://docs.microsoft.com/en-us/azure/firewall/overview  Network security groups  https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview |
|  |  | We have a zero-trust networking model. We do not have a Firewall in Azure. We do not use NSG. |  |  |  |
|  |  | We have a zero-trust networking model. We only use Azure Firewall / Third-party Firewall to protect our network. |  |  |  |
|  |  | We have a zero-trust networking model. We have network segmentation. We use Azure Firewall with Azure Firewall Manager, Azure NSG on each subnet/nic. |  |  |  |
| **NET10** | How do you perform packet inspection in Azure? |  | In many industries, organizations require that traffic in Azure is mirrored to a network packet collector for deep inspection and analysis. This requirement typically focuses on inbound and outbound internet traffic. This section explores key considerations and recommended approaches for mirroring or tapping traffic within Azure Virtual Network. | Azure virtual network TAP (Terminal Access Point) allows you to continuously stream your virtual machine network traffic to a network packet collector or analytics tool. The collector or analytics tool is provided by a network virtual appliance partner. For a list of partner solutions that are validated to work with virtual network TAP, see partner solutions. The following picture shows how virtual network TAP works. You can add a TAP configuration on a network interface that is attached to a virtual machine deployed in your virtual network. The destination is a virtual network IP address in the same virtual network as the monitored network interface or a peered virtual network. The collector solution for virtual network TAP can be deployed behind an Azure Internal Load balancer for high availability.  As an alternative to Azure Virtual Network TAP, evaluate the following options:  Use Network Watcher packets to capture despite the limited capture window.  Evaluate if the latest version of NSG flow logs provides the level of detail that you need.  Use partner solutions for scenarios that require deep packet inspection.  Don't develop a custom solution to mirror traffic. Although this approach might be acceptable for small-scale scenarios, we don't encourage it at scale because of complexity and the supportability issues that might arise.  Network security groups (NSG) allow or deny inbound or outbound traffic to a network interface in a VM. The NSG flow log capability allows you to log the source and destination IP address, port, protocol, and whether traffic was allowed or denied by an NSG. You can analyze logs using a variety of tools, such as PowerBI and the traffic analytics capability. Traffic analytics provides rich visualizations of data written to NSG flow logs. | What is Azure Network Watcher?  https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview  Virtual network TAP  https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-tap-overview  Network topology and connectivity  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/network-topology-and-connectivity |
|  |  | We use a custom solution to capture network logs. |  |  |  |
|  |  | We capture logs from our Azure Firewall / Third-party Firewall. |  |  |  |
|  |  | We capture logs from our Azure Firewall / Third-party Firewall. We have enabled NSG flow logs and enabled alert rules for most important scenarios. |  |  |  |

* 1. Additional findings and Recommendations

1. Management and Monitoring
   1. Assessment details

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Label | Question | Answer | Why consider this | Suggested Actions | Learn More |
| **MM01** | What is the current logging, monitoring and alerting solution for your workloads in Azure and on-premises environments? |  | The enterprise-scale architecture approach advocates using Azure-native platform services and capabilities whenever possible. This approach should align with Azure platform roadmaps to ensure that new capabilities are available within your environments. Azure platform roadmaps should help to inform the migration strategy and enterprise-scale trajectory.  Azure Monitor can collect data from a variety of sources. You can think of monitoring data for your applications in tiers ranging from your application, any operating system, and services it relies on, down to the platform itself. Azure Monitor collects data from each of the following tiers:  Application monitoring data: Data about the performance and functionality of the code you have written, regardless of its platform.  Guest OS monitoring data: Data about the operating system on which your application is running. This could be running in Azure, another cloud, or on-premises.  Azure resource monitoring data: Data about the operation of an Azure resource.  Azure subscription monitoring data: Data about the operation and management of an Azure subscription, as well as data about the health and operation of Azure itself.  Azure tenant monitoring data: Data about the operation of tenant-level Azure services, such as Azure Active Directory. | Use a centralized Azure Monitor Log Analytics workspace to collect logs and metrics from IaaS and PaaS app resources and control log access with RBAC.  Use Azure Monitor metrics for time-sensitive analysis. Metrics in Azure Monitor are stored in a time-series database optimized to analyze time-stamped data. These metrics are well suited for alerts and detecting issues quickly. They can also tell you how your system is performing. They typically need to be combined with logs to identify the root cause of issues.  Use Azure Monitor logs for insights and reporting. Logs contain different types of data that's organized into records with different sets of properties. They're useful for analyzing complex data from a range of sources, such as performance data, events, and traces.  When necessary, use shared storage accounts within the landing zone for Azure diagnostic extension log storage.  Alerts proactively notify you when issues are found with your infrastructure or application using your monitoring data in Azure Monitor. They allow you to identify and address issues before the users of your system notice them.  Use Azure Monitor alerts for the generation of operational alerts. Azure Monitor alerts unify alerts for metrics and logs and use features such as action and smart groups for advanced management and remediation purposes. | Azure Monitor overview  https://docs.microsoft.com/en-us/azure/azure-monitor/overview  Management and monitoring  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/management-and-monitoring |
|  |  | third-party Monitoring solutions are in use to monitor, detect and generate alerts for On-Premises and IaaS environments. There are no Cloud-based services monitoring at this moment. |  |  |  |
|  |  | On-Premises and IaaS monitoring and alerts are detected by SCOM or a third-party monitoring solution. Cloud-based services monitoring is based on **Azure Monitor**. Monitoring overall strategy does not have a single and cohesive solution. |  |  |  |
|  |  | Azure Monitor is used for cloud services and on-premises. Alerts are centrally managed and generated from a single solution. We use a single Log Analytics workspace for centralized platform management except where RBAC, retention of data types and data sovereignty requirements mandate the consideration of separate workspaces. |  |  |  |
| **MM02** | What is the solution for visualizing monitoring data? |  | Use operational dashboards using cloud native tools such as Azure Monitor logs or third-party tooling. | Use Azure Monitor logs for insights and reporting. Logs contain different types of data that's organized into records with different sets of properties. They're useful for analyzing complex data from a range of sources, such as performance data, events, and traces.  Workbooks in Azure Monitor provide a flexible canvas for data analysis and the creation of rich visual reports within the Azure portal. They allow you to tap into multiple data sources from across Azure and combine them into unified interactive experiences.  Workbooks can query data from multiple sources within Azure. Authors of workbooks can transform this data to provide insights into the availability, performance, usage, and overall health of the underlying components. For instance, analyzing performance logs from virtual machines to identify high CPU or low memory instances and displaying the results as a grid in an interactive report.  But the real power of workbooks is the ability to combine data from disparate sources within a single report. This allows for the creation of composite resource views or joins across resources enabling richer data and insights that would otherwise be impossible.  To maintain your existing investment in System Center Operations Manager and use extended capabilities with Azure Monitor, you can integrate Operations Manager with your Log Analytics workspace. This allows you to leverage the opportunities of logs in Azure Monitor while continuing to use Operations Manager to:  Monitor the health of your IT services with Operations Manager  Maintain integration with your ITSM solutions supporting incident and problem management  Manage the lifecycle of agents deployed to on-premises and public cloud IaaS virtual machines that you monitor with Operations Manager  Integrating with System Center Operations Manager adds value to your service operations strategy by using the speed and efficiency of Azure Monitor in collecting, storing, and analyzing log data from Operations Manager. Azure Monitor log queries help correlate and work towards identifying the faults of problems and surfacing recurrences in support of your existing problem management process. The flexibility of the query engine to examine performance, event, and alert data, with rich dashboards and reporting capabilities to expose this data in meaningful ways, demonstrates the strength Azure Monitor brings in complimenting Operations Manager. | Azure Monitor overview  https://docs.microsoft.com/en-us/azure/azure-monitor/overview  Management and monitoring  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/management-and-monitoring  Connect Operations Manager to Azure Monitor  https://docs.microsoft.com/en-us/azure/azure-monitor/platform/om-agents |
|  |  | Default Dashboards from SCOM or a third-party monitoring solution are the only visualizations the customer has at this moment. These Dashboards only provide information for On-Premises and IaaS environments. |  |  |  |
|  |  | Customized Dashboards for SCOM or a third-party monitoring solution have been developed for On-Premises and IaaS environments. **Azure Monitor Workbooks** for some PaaS services have been developed. |  |  |  |
|  |  | Azure Monitor Workbooks are heavily used to centralize all the organization environments including On-Premises and Cloud based services. |  |  |  |
| **MM03** | Do you use any tool that proactively identifies potential optimizations of your Cloud environment? |  | Azure Advisor provides best practice recommendations for your workloads. These recommendations are personalized and actionable to help you:  Improve the posture of your workloads and optimize your Azure deployments  Proactively prevent top issues by following best practices  Assess your Azure workloads against the five pillars of the Microsoft Azure Well-Architected Framework | Use Azure Advisor to get cost, performance, security, high availability, and operational excellence recommendations of your current workloads.  Use Azure Advisor Score to help you achieve these goals effectively and efficiently.  Whenever Azure Advisor detects a new recommendation for one of your resources, an event is stored in Azure Activity log. Set up alerts for these events from Azure Advisor using a recommendation-specific alerts creation experience. You can select a subscription and optionally a resource group to specify the resources that you want to receive alerts on. | Introduction to Azure Advisor  https://docs.microsoft.com/en-us/azure/advisor/advisor-overview |
|  |  | No. We rely on professional services to identify recommendations and optimization once a year. Continuous Optimization monitoring is not implemented nor adopted. |  |  |  |
|  |  | We are aware of Azure **Advisor** and review the recommendations from time to time, but we do not have processes and operations around it to continuously optimize their Cloud resources. |  |  |  |
|  |  | We have process and operations to leverage Azure Advisor recommendations periodically and configured alerts to receive notification and act on recommendations automatically. |  |  |  |
| **MM04** | How do you onboard Azure resources for management and monitoring? |  | Using Azure Policy, you can onboard virtual machines and Azure resources with Azure Monitor automatically for current workload and resources that will be added in future. | Use Azure Policy for access control and compliance reporting. Azure Policy provides the ability to enforce organization-wide settings to ensure consistent policy adherence and fast violation detection. For more information, see Understand Azure Policy effects.  Use update management in Azure Automation as a long-term patching mechanism for both Windows and Linux VMs. Enforcing update management configurations through policy ensures that all VMs are included in the patch management regimen and provides application teams with the ability to manage patch deployment for their VMs. It also provides visibility and enforcement capabilities to the central IT team across all VMs.  Use Azure Policy allows to install the required agents for Azure Monitor for VMs and to enable diagnostics settings and log collection in Azure resources.  Use a centralized Azure Monitor Log Analytics workspace to collect logs and metrics from IaaS and PaaS app resources and control log access with RBAC. | Deploy Azure Monitor at scale using Azure Policy  https://docs.microsoft.com/en-us/azure/azure-monitor/deploy-scale  Enable Azure Monitor for VMs by using Azure Policy  https://docs.microsoft.com/en-us/azure/azure-monitor/insights/vminsights-enable-policy  Management and monitoring  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/management-and-monitoring" |
|  |  | We install monitoring agents and configure the diagnostics settings on Azure resources manually. |  |  |  |
|  |  | We use Azure **Policy** to deploy monitoring agents and diagnostic settings for some Azure resources, but configuration is not consistent across all Azure resources. |  |  |  |
|  |  | We enable guest configuration audit capabilities through policy. This provides our application teams with the ability to immediately consume the feature capabilities for their workloads with very little effort. |  |  |  |
| **MM05** | How do you manage logs and telemetry centralized? |  | IT organizations today are modeled following either a centralized, decentralized, or an in-between hybrid of both structures. As a result, the following workspace deployment models have been commonly used to map to one of these organizational structures:  Centralized: All logs are stored in a central workspace and administered by a single team, with Azure Monitor providing differentiated access per-team. In this scenario, it is easy to manage, search across resources, and cross-correlate logs. The workspace can grow significantly depending on the amount of data collected from multiple resources in your subscription, with additional administrative overhead to maintain access control to different users. This model is known as "hub and spoke".  Decentralized: Each team has their own workspace created in a resource group they own and manage, and log data is segregated per resource. In this scenario, the workspace can be kept secure and access control is consistent with resource access, but it's difficult to cross-correlate logs. Users who need a broad view of many resources cannot analyze the data in a meaningful way.  Hybrid: Security audit compliance requirements further complicate this scenario because many organizations implement both deployment models in parallel. This commonly results in a complex, expensive, and hard-to-maintain configuration with gaps in logs coverage.  In the context of the enterprise-scale architecture, centralized logging is primarily concerned with platform operations. This emphasis doesn't prevent the use of the same workspace for VM-based application logging. With a workspace configured in resource-centric access control mode, granular RBAC is enforced to ensure app teams will only have access to the logs from their resources. In this model, app teams benefit from the use of existing platform infrastructure by reducing their management overhead. For any non-compute resources such as web apps or Azure Cosmos DB databases, application teams can use their own Log Analytics workspaces and configure diagnostics and metrics to be routed here. | Use an Azure Monitor Log Analytics workspace as an administrative boundary.  Don't send raw log entries back to on-premises monitoring systems. Instead, adopt a principle that data born in Azure stays in Azure. If on-premises SIEM integration is required, then send critical alerts instead of logs.  Use a single monitor logs workspace to manage platforms centrally except where role-based access control (RBAC), data sovereignty requirements and data retention policies mandate separate workspaces. Centralized logging is critical to the visibility required by operations management teams. Logging centralization drives reports about change management, service health, configuration, and most other aspects of IT operations. Converging on a centralized workspace model reduces administrative effort and the chances for gaps in observability. | Management and monitoring  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/management-and-monitoring  Designing your Azure Monitor Logs deployment  https://docs.microsoft.com/en-us/azure/azure-monitor/platform/design-logs-deployment |
|  |  | We capture logs from few applications and services in Azure. |  |  |  |
|  |  | We have integration with on-premises security information and event management (**SIEM**) systems such as ServiceNow or ArcSight. We send all raw data to our on-premises SIEM system. |  |  |  |
|  |  | We have integration with on-premises security information and event management (SIEM) systems such as ServiceNow or ArcSight. We do not send raw log entries back to on-premises monitoring systems. Instead, we have adopted a principle that data born in Azure stays in Azure. If on-premises SIEM integration is required, then we send critical alerts instead of logs. |  |  |  |
| **MM06** | How do you handle Azure data retention thresholds and archiving requirements? |  | Azure data retention thresholds and archiving requirements:  The default retention period for Azure Monitor logs is 30 days, with a maximum of two years.  The default retention period for Azure AD reports (premium) is 30 days.  The default retention period for the Azure diagnostic service is 90 days. | Use an Azure Monitor Log Analytics workspace as an administrative boundary.  Use a single monitor logs workspace to manage platforms centrally except where role-based access control (RBAC), data sovereignty requirements and data retention policies mandate separate workspaces. Centralized logging is critical to the visibility required by operations management teams. Logging centralization drives reports about change management, service health, configuration, and most other aspects of IT operations. Converging on a centralized workspace model reduces administrative effort and the chances for gaps in observability.  In the context of the enterprise-scale architecture, centralized logging is primarily concerned with platform operations. This emphasis doesn't prevent the use of the same workspace for VM-based application logging. With a workspace configured in resource-centric access control mode, granular RBAC is enforced to ensure app teams will only have access to the logs from their resources. In this model, app teams benefit from the use of existing platform infrastructure by reducing their management overhead. For any non-compute resources such as web apps or Azure Cosmos DB databases, application teams can use their own Log Analytics workspaces and configure diagnostics and metrics to be routed here.  Export logs to Azure Storage if log retention requirements exceed two years. Use immutable storage with a write-once, read-many policy to make data non-erasable and non-modifiable for a user-specified interval. | Management and monitoring  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/management-and-monitoring |
|  |  | We use default retention period for Azure diagnostic service, Azure Monitor and Azure Active Directory Logs. |  |  |  |
|  |  | We know the default retention period for Azure diagnostic service, Azure Monitor and Azure Active Directory Logs and we have configured **Azure Log Analytics retention** based on our retention requirements. |  |  |  |
|  |  | We know the default retention period for Azure diagnostic service, Azure Monitor and Azure Active Directory Logs and we have configured Azure Log Analytics retention based on our retention requirements. We export logs to Azure Storage if log retention requirements exceed 2 years. We leverage immutable storage with WORM policy (Write Once, Read Many) to make data non-erasable and non-modifiable for a user-specified interval. |  |  |  |
| **MM07** | How do you use Azure Services Health? |  | Service Health provides you with a customizable dashboard which tracks the health of your Azure services in the regions where you use them. In Azure Service Health dashboard, you can track active events like ongoing service issues, upcoming planned maintenance, or relevant health advisories. When events become inactive, they get placed in your health history for up to 90 days. Finally, you can use the Service Health dashboard to create and manage service health alerts which proactively notify you when service issues are affecting you.  Service Health integrates with Azure Monitor to alert you via emails, text messages, and webhook notifications when your business-critical resources are impacted. Set up an activity log alert for the appropriate service health event. Route that alert to the appropriate people in your organization using Action Groups.  Azure Resource Health helps you diagnose and get support for service problems that affect your Azure resources. It reports on the current and past health of your resources. | Include service and resource health events as part of the overall platform monitoring solution. Tracking service and resource health from the platform perspective is an important component of resource management in Azure.  Use a single monitor logs workspace to manage platforms centrally except where role-based access control (RBAC), data sovereignty requirements and data retention policies mandate separate workspaces. Centralized logging is critical to the visibility required by operations management teams. Logging centralization drives reports about change management, service health, configuration, and most other aspects of IT operations. Converging on a centralized workspace model reduces administrative effort and the chances for gaps in observability. | Service Health overview  https://docs.microsoft.com/en-us/azure/service-health/service-health-overview  Resource Health overview  https://docs.microsoft.com/en-us/azure/service-health/resource-health-overview  Management and monitoring  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/management-and-monitoring |
|  |  | We do not use Azure resource health events. We act based on users’ feedback and reactively try to mitigate the impact or accelerate the solution. |  |  |  |
|  |  | We proactively review **Azure Service Health notifications** and take action to mitigate the impact. |  |  |  |
|  |  | We leverage Azure Service Health capabilities to customize alerts and proactively get notifications about current or upcoming Cloud Services outages. We have logging centralization about change management, service health, configuration, and most other aspects of IT operations. Converging on a centralized workspace model reduces administrative effort and the chances for gaps in observability. |  |  |  |
| **MM08** | Do you have monitoring solutions to manage usage, performance, and failures of your Cloud applications? |  | Application-centric platform monitoring, encompassing both hot and cold telemetry paths for metrics and logs, respectively:  Operating system metrics; for example, performance counters and custom metrics  Operating system logs; for example, Internet Information Services, Event Tracing for Windows, and syslogs  Resource health events | Use Azure Monitor to gain an insight into how your applications are functioning. Monitoring is a crucial part of maintaining quality-of-service targets. Common scenarios for collecting monitoring data include:  Ensuring that the system remains healthy.  Tracking the availability of the system and its component elements.  Maintaining performance to ensure that the throughput of the system does not degrade unexpectedly as the volume of work increases.  Guaranteeing that the system meets any service-level agreements (SLAs) established with customers.  Protecting the privacy and security of the system, users, and their data.  Tracking the operations that are performed for auditing or regulatory purposes.  Monitoring the day-to-day usage of the system and spotting trends that might lead to problems if they're not addressed.  Tracking issues that occur, from initial report through to analysis of possible causes, rectification, consequent software updates, and deployment.  Tracing operations and debugging software releases. | Best practices for monitoring cloud applications  https://docs.microsoft.com/en-us/azure/architecture/best-practices/monitoring  Management and monitoring  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/management-and-monitoring |
|  |  | We are using third-party tool to monitor applications in cloud and on-premises environment. |  |  |  |
|  |  | We use **Azure Monitor Application Insights** to get detailed information and analytics certain critical cloud applications. |  |  |  |
|  |  | We have established an application-centric platform monitoring model that is encompassing both hot and cold telemetry paths for metrics and logs. For application monitoring we use dedicated Log Analytics workspaces so we can allow our application teams access the logs using RBAC they have on their applications/virtual machines. |  |  |  |
| **MM09** | Do you use Azure Resource Lock to prevent accidental deletion of critical shared service? |  | As an administrator, you may need to lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources. You can set the lock level to CanNotDelete or ReadOnly. In the portal, the locks are called Delete and Read-only respectively.  CanNotDelete means authorized users can still read and modify a resource, but they can't delete the resource.  ReadOnly means authorized users can read a resource, but they can't delete or update the resource. Applying this lock is like restricting all authorized users to the permissions granted by the Reader role. | Use resource locks to prevent accidental deletion of critical shared services. | Lock resources to prevent unexpected changes  https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources  Management and monitoring  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/management-and-monitoring |
|  |  | No. |  |  |  |
|  |  | Yes. We assign Azure Resource **Lock** manually to critical or shared resources as required. |  |  |  |
|  |  | Yes. We assign Azure Resource Lock automatically when the resources are deployed to critical or shared resources. |  |  |  |
| **MM10** | What is your patch management strategy for IaaS workloads in Azure? |  | You can use Update Management in Azure Automation to manage operating system updates for your Windows and Linux machines in Azure, in on-premises environments, and in other cloud environments. You can quickly assess the status of available updates on all agent machines and manage the process of installing required updates for servers. | Use update management in Azure Automation as a long-term patching mechanism for both Windows and Linux VMs. Enforcing update management configurations through policy ensures that all VMs are included in the patch management regimen and provides application teams with the ability to manage patch deployment for their VMs. It also provides visibility and enforcement capabilities to the central IT team across all VMs. | Update Management overview  https://docs.microsoft.com/en-us/azure/automation/update-management/update-mgmt-overview  Management and monitoring  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/management-and-monitoring |
|  |  | We do not manage automatic patching for Azure workloads. Patches are applied to VMs as needed by workload owners. / We use a third-party solution for patch management for our IaaS (Windows and Linux) VMs in Azure. |  |  |  |
|  |  | We use **Update Management in Azure Automation** as a long-term patching mechanism, for both Windows and Linux VMs. We onboard VMs to Azure Update Management manually. |  |  |  |
|  |  | "We use Update Management in Azure Automation as a long-term patching mechanism, for both Windows and Linux VMs. |  |  |  |
| **MM11** | Do you have any monitoring solution to discover application components and maps the communication between them to show connections between servers and processes? |  | You can use monitoring to gain an insight into how well a system is functioning. Monitoring is a crucial part of maintaining quality-of-service targets. Common scenarios for collecting monitoring data include:  Ensuring that the system remains healthy.  Tracking the availability of the system and its component elements.  Maintaining performance to ensure that the throughput of the system does not degrade unexpectedly as the volume of work increases.  Guaranteeing that the system meets any service-level agreements (SLAs) established with customers.  Protecting the privacy and security of the system, users, and their data.  Tracking the operations that are performed for auditing or regulatory purposes.  Monitoring the day-to-day usage of the system and spotting trends that might lead to problems if they're not addressed.  Tracking issues that occur, from initial report through to analysis of possible causes, rectification, consequent software updates, and deployment.  Tracing operations and debugging software releases.  Application monitoring can use dedicated Log Analytics workspaces.  For applications that are deployed to virtual machines, logs should be stored centrally to the dedicated Log Analytics workspace from a platform perspective. Application teams can access the logs subject to the RBAC they have on their applications or virtual machines.  App performance and health monitoring for both infrastructure as a service (IaaS) and platform as a service (PaaS) resources.  Data aggregation across all app components.  Health modeling and operationalization:  How to measure the health of the workload and its subsystems  A traffic-light model to represent health  How to respond to failures across app components | Distributed applications and services running in the cloud are, by their nature, complex pieces of software that comprise many moving parts. In a production environment, it's important to be able to track the way in which users use your system, trace resource utilization, and generally monitor the health and performance of your system. You can use this information as a diagnostic aid to detect and correct issues, and also to help spot potential problems and prevent them from occurring.  Use a centralized Azure Monitor Log Analytics workspace to collect logs and metrics from IaaS and PaaS app resources and control log access with RBAC.  Use Azure Monitor metrics for time-sensitive analysis. Metrics in Azure Monitor are stored in a time-series database optimized to analyze time-stamped data. These metrics are well suited for alerts and detecting issues quickly. They can also tell you how your system is performing. They typically need to be combined with logs to identify the root cause of issues.  Use Azure Monitor logs for insights and reporting. Logs contain different types of data that's organized into records with different sets of properties. They're useful for analyzing complex data from a range of sources, such as performance data, events, and traces.  When necessary, use shared storage accounts within the landing zone for Azure diagnostic extension log storage.  Use Azure Monitor alerts for the generation of operational alerts. Azure Monitor alerts unify alerts for metrics and logs and use features such as action and smart groups for advanced management and remediation purposes.  Use Azure Application Map to help you to spot performance bottlenecks or failure hotspots across all components of your distributed application. Each node on the map represents an application component or its dependencies; and has health KPI and alerts status. You can click through from any component to more detailed diagnostics, such as Application Insights events. If your app uses Azure services, you can also click through to Azure diagnostics, such as SQL Database Advisor recommendations. | Best practices for monitoring cloud applications  https://docs.microsoft.com/en-us/azure/architecture/best-practices/monitoring  Management and monitoring  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/management-and-monitoring  Application Map: Triage Distributed Applications  https://docs.microsoft.com/en-us/azure/azure-monitor/app/app-map?tabs=net |
|  |  | Application Services Maps exists but are manually generated based on the application development teams. Communication between the components is not tracked with monitoring tools but is assumed. |  |  |  |
|  |  | We are conducting some tests with **Azure Service Maps** for some applications but processes and operations around it are not defined |  |  |  |
|  |  | We use Azure Service Maps as part of their Monitoring strategy to identify dependencies and connections between components of IaaS applications |  |  |  |

* 1. Additional findings and Recommendations

1. Business Continuity and Disaster Recovery
   1. Assessment details

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Label | Question | Answer | Why consider this | Suggested Actions | Learn More |
| **BC01** | What is the current approach and solution to keep your data safe and recoverable? |  | Use Azure-native backup capabilities.  Azure Backup and PaaS-native backup features remove the need for managing third-party backup software and infrastructure. As with other native features, you can set, audit, and enforce backup configurations with Azure Policy. This ensures that services remain compliant with the organization's requirements. | Use Azure-native backup capabilities. Azure Backup comprehensively protects your data assets in Azure through a simple, secure, and cost-effective solution that requires zero-infrastructure. It's Azure's built-in data protection solution for a wide range of workloads. It helps protect your mission critical workloads running in the cloud, and ensures your backups are always available and managed at scale across your entire backup estate.  Azure Backup enables data protection for various workloads (on-premises and cloud). It's a secure and reliable built-in data protection mechanism in Azure. It can seamlessly scale its protection across multiple workloads without any management overhead for you. There are multiple automation channels as well to enable this (via PowerShell, CLI, Azure Resource Manager templates, and REST APIs.)  Scalable, durable, and secure storage - Azure Backup uses reliable Blob storage with in-built security and high availability features. You can choose LRS, GRS, or RA-GRS storages for your backup data.  Native workload integration - Azure Backup provides native integration with Azure Workloads (VMs, SAP HANA, SQL in Azure VMs and even Azure Files) without requiring you to manage automation or infrastructure to deploy agents, write new scripts or provision storage.  Azure Backup uses vaults (Recovery Services and Backup vaults) to orchestrate and manage backups. It also uses vaults to store backed-up data. Effective vault design helps organizations establish a structure to organize and manage backup assets in Azure to support your business priorities. Since the vault is scoped to a subscription, fit your vault design to meet the subscription design strategy such as Application category strategy where subscriptions are separated based on specific applications or services or along the lines of application archetypes.  Consider grouping VMs that require the same schedule start time, frequency, and retention settings within a single policy.  Ensure the backup scheduled start time is during non-peak production application time.  To distribute backup traffic, consider backing up different VMs at different times of the day and make sure the times don't overlap.  If your workloads are all managed by a single subscription and single resource, then you can use a single vault to monitor and manage your backup estate.  If your workloads are spread across subscriptions, then you can create multiple vaults, one or more per subscription.  Backup Center allows you to have a single pane of glass to manage all tasks related to Backup. Learn more here.  You can customize your views with workbook templates. Backup Explorer is one such template for Azure VMs. Learn more here.  If you needed consistent policy across vaults, then you can use Azure policy to propagate backup policy across multiple vaults. You can write a custom Azure Policy definition that uses the ‘deployIfNotExists’ effect to propagate a backup policy across multiple vaults. You assign can assign this Azure Policy definition to a particular scope (subscription or RG), so that it deploys a 'backup policy' resource to all Recovery Services vaults in the scope of the Azure Policy assignment. The settings of the backup policy (such as backup frequency, retention, and so on) should be specified by the user as parameters in the Azure Policy assignment.  As your organizational footprint grows, you might want to move workloads across subscriptions for the following reasons: align by backup policy, consolidate vaults, trade-off on lower redundancy to save on cost (move from GRS to LRS). Azure Backup supports moving a Recovery Services vault across Azure subscriptions, or to another resource group within the same subscription. | Backup cloud and on-premises workloads to cloud  https://docs.microsoft.com/en-us/azure/backup/guidance-best-practices  Enterprise-scale business continuity and disaster recovery  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/business-continuity-and-disaster-recovery |
|  |  | we use 3rd party tools to back up data to datacenters within region. |  |  |  |
|  |  | we use 3rd party tools to back up data and applications to different datacenters in different regions. |  |  |  |
|  |  | we use Azure Backup /Azure Site Recovery to back on-prem and cloud workloads. |  |  |  |
| **BC02** | Do you have backup strategies and solutions for on-premises, IaaS and PaaS workloads? |  | Azure Backup and PaaS-native backup features remove the need for managing third-party backup software and infrastructure. As with other native features, you can set, audit, and enforce backup configurations with Azure Policy. This ensures that services remain compliant with the organization's requirements. | Use Azure-native backup capabilities:  Azure Backup and PaaS-native backup features remove the need for managing third-party backup software and infrastructure. As with other native features, you can set, audit, and enforce backup configurations with Azure Policy. This ensures that services remain compliant with the organization's requirements.  Azure Backup and PaaS-native backup features remove the need for managing third-party backup software and infrastructure. As with other native features, you can set, audit, and enforce backup configurations with Azure Policy. This ensures that services remain compliant with the organization's requirements.  Define your applications and data availability requirements, and the use of active-active and active-passive availability patterns (such as workload RTO and RPO requirements). | Backup cloud and on-premises workloads to cloud  https://docs.microsoft.com/en-us/azure/backup/guidance-best-practices  Enterprise-scale business continuity and disaster recovery  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/business-continuity-and-disaster-recovery |
|  |  | On-Premises and IaaS Backup is fully managed by 3rd Party solutions, on premises data backup stored |  |  |  |
|  |  | On-Premises and IaaS Backup are fully managed by 3rd Party solutions and copies are stored in Azure. PaaS Services Backup strategy is not defined yet. |  |  |  |
|  |  | On-Premises and IaaS Backups are fully managed using Azure Backup. PaaS backup strategy is based on per Azure service availability. For example, for SQL the customer is leveraging the inbox solution provided in Azure SQL managed instances |  |  |  |
| **BC03** | Does your business model and applications require a multi-region always on availability? What pattern better describes your business requirements? (Active/Passive, Active/Active or both)? |  | Your organization or enterprise needs to design suitable, platform-level capabilities that application workloads can consume to meet their specific requirements. Specifically, these application workloads have requirements pertaining to recover time objective (RTO) and recovery point objective (RPO). Be sure that you capture disaster recovery (DR) requirements to design capabilities appropriately for these workloads. | Employ Azure Site Recovery for Azure-to-Azure Virtual Machines disaster recovery scenarios. This enables you to replicate workloads across regions.  Site Recovery provides built-in platform capabilities for VM workloads to meet low RPO/RTO requirements through real-time replication and recovery automation. Additionally, the service provides the ability to run recovery drills without affecting the workloads in production. You can use Azure Policy to enable replication and also audit the protection of your VMs.  Use multiple regions and peering locations for ExpressRoute connectivity.  A redundant hybrid network architecture can help ensure uninterrupted cross-premises connectivity in the event of an outage affecting an Azure region or peering provider location.  Avoid using overlapping IP address ranges for production and DR sites.  When possible, plan for a business continuity and DR network architecture that provides concurrent connectivity to all sites. DR networks that use the same classless inter-domain routing blocks, such as production networks, require a network failover process that can complicate and delay application failover in the event of an outage | About Site Recovery  https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-overview  Enterprise-scale business continuity and disaster recovery  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/business-continuity-and-disaster-recovery |
|  |  | 2 or more Azure regions are used for Cloud Based services, however Active/Active and/or Active/Passive and load balancing architectures have not been implemented. |  |  |  |
|  |  | 2 or more Azure regions are in use to protect in Active/passive mode the existing IaaS workloads. PaaS workloads are not replicated, or load balanced between regions |  |  |  |
|  |  | 2 or more Azure regions are in use to protect in Active/Passive mode the existing IaaS workloads. PaaS active/active protection and load balancing is enabled for certain services like DNS or web applications |  |  |  |
| **BC04** | Do you have a clear definition of your services SLAs, RTO and RPOs? |  | Every design decision must be justified by a business requirement  This design principle may seem obvious, but it's crucial to keep in mind when designing a solution. Do you anticipate millions of users, or a few thousand? Is a one-hour application outage acceptable? Do you expect large bursts in traffic or a predictable workload? Ultimately, every design decision must be justified by a business requirement. | Define and document service level agreements (SLA) and service level objectives (SLO), including availability and performance metrics. You might build a solution that delivers 99.95% availability. Is that enough? The answer is a business decision.  Define business objectives, including the recovery time objective (RTO), recovery point objective (RPO), and maximum tolerable outage (MTO). These numbers should inform decisions about the architecture. For example, to achieve a low RTO, you might implement automated failover to a secondary region. But if your solution can tolerate a higher RTO, that degree of redundancy might be unnecessary.  Define your applications and data availability requirements, and the use of active-active and active-passive availability patterns (such as workload RTO and RPO requirements). | Service Level Agreements  https://azure.microsoft.com/en-us/support/legal/sla/  Build for the needs of the business  https://docs.microsoft.com/en-us/azure/architecture/guide/design-principles/build-for-business  Enterprise-scale business continuity and disaster recovery  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/business-continuity-and-disaster-recovery |
|  |  | We have expectation of higher SLAs in Azure. |  |  |  |
|  |  | We take backup and enabled replication of VMs in Azure, but we have not defined RPOs or RTOs yet. |  |  |  |
|  |  | We have a clear definition of our SLAs, RTOs and RPOs. We take backup and enabled replication of VMs in Azure to meet these goals. |  |  |  |
| **DR01** | How do you manage disaster recovery for IaaS workloads in Azure? |  | Site Recovery provides built-in platform capabilities for VM workloads to meet low RPO/RTO requirements through real-time replication and recovery automation. Additionally, the service provides the ability to run recovery drills without affecting the workloads in production. You can use Azure Policy to enable replication and audit the protection of your VMs. | Employ Azure Site Recovery for Azure-to-Azure Virtual Machines disaster recovery scenarios. This enables you to replicate workloads across regions.  Site Recovery provides built-in platform capabilities for VM workloads to meet low RPO/RTO requirements through real-time replication and recovery automation. Additionally, the service provides the ability to run recovery drills without affecting the workloads in production. You can use Azure Policy to enable replication and also audit the protection of your VMs. | Azure to Azure disaster recovery architecture  https://docs.microsoft.com/en-us/azure/site-recovery/azure-to-azure-architecture  Enterprise-scale business continuity and disaster recovery  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/business-continuity-and-disaster-recovery |
|  |  | We use a third-part tool for our DR scenario. |  |  |  |
|  |  | We have enabled Azure Site Recovery for some VMs in Azure. we do not have a strategy defined yet. |  |  |  |
|  |  | We have set up Azure to Azure Site recovery, tested failover and defined a clear procedure to use in case a failover is needed. We use Azure policy to audit and deploy VM replication. |  |  |  |
| **DR02** | How do you manage disaster recovery for PaaS workloads in Azure? |  | Azure built-in features provide an easy solution to the complex task of building replication and failover into a workload architecture, simplifying both design and deployment automation. An organization that has defined a standard for the services they use can also audit and enforce the service configuration through Azure Policy.  Define your business continuity and DR requirements for platform as a service (PaaS) services, and the availability of native DR and high-availability features. | Use native PaaS service disaster recovery capabilities.  Use geo-replication and DR capabilities for PaaS services. | Enterprise-scale business continuity and disaster recovery  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/business-continuity-and-disaster-recovery |
|  |  | We only use PaaS services in one region in Azure. |  |  |  |
|  |  | For some workloads we have enabled geo replication in Azure. |  |  |  |
|  |  | We use Azure geo replication for some of our PaaS services, e.g., Azure SQL DB, Storage Accounts. We use Azure Policy to audit resources that do not have the replication enabled. |  |  |  |

* 1. Additional findings and Recommendations

1. Security, Governance, and Compliance
   1. Assessment details

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Label | Question | Answer | Why consider this | Suggested Actions | Learn More |
| **SE01** | Are your development teams adhering and adopting a set of practices that support security assurance and compliance requirements such as Microsoft's Security Development Lifecycle (SDL) to build highly secure software, address security compliance requirements, and reduce development costs? |  | Your organization might have a formal application security program that assists you with security activities from start to finish during the development lifecycle. If your organization has security and compliance teams, be sure to engage them before you begin developing your application. Ask them at each phase of the SDL whether there are any tasks you missed. | Use the following resources to learn more about developing secure applications and to help secure your applications on Azure:  Microsoft Security Development Lifecycle (SDL) – The SDL is a software development process from Microsoft that helps developers build more secure software. It helps you address security compliance requirements while reducing development costs.  Open Web Application Security Project (OWASP) – OWASP is an online community that produces freely available articles, methodologies, documentation, tools, and technologies in the field of web application security.  Pushing Left, like a Boss – A series of online articles that outlines different types of application security activities that developers should complete to create more secure code.  Microsoft identity platform – The Microsoft identity platform is an evolution of the Azure AD identity service and developer platform. It’s a full-featured platform that consists of an authentication service, open-source libraries, application registration and configuration, full developer documentation, code samples, and other developer content. The Microsoft identity platform supports industry-standard protocols like OAuth 2.0 and OpenID Connect.  Security best practices for Azure solutions – A collection of security best practices to use when you design, deploy, and manage cloud solutions by using Azure. This paper is intended to be a resource for IT pros. This might include designers, architects, developers, and testers who build and deploy secure Azure solutions.  Security and Compliance Policy on Azure – Azure Security and Compliance Policy are resources that can help you build and launch cloud-powered applications that comply with stringent regulations and standards. | Secure development best practices on Azure  https://docs.microsoft.com/en-us/azure/security/develop/secure-dev-overview  " |
|  |  | Microsoft SDL framework is not used by development teams or DevOps teams. Security requirements for software development exists mainly as organizational knowledge and recommendations given by IT Security on request |  |  |  |
|  |  | SDL is partially in use but advanced practices like penetration testing and attack surface review are not enforced nor implemented |  |  |  |
|  |  | Microsoft SDL framework and recommendations are enforced by the organization. |  |  |  |
| **SE02** | Are you integrating detection and response capabilities into DevOps practices such as early security checks on CI/CD pipeline and security monitoring in operation? |  | DevOps practices are allowing businesses to stay ahead of the competition by delivering new features faster than ever before. As the frequency of production deployments increases, this business agility cannot come at the expense of security. With continuous delivery, how do you ensure your applications are secure and stay secure? How can you find and fix security issues early in the process? This begins with practices commonly referred to as DevSecOps. DevSecOps incorporates the security team and their capabilities into your DevOps practices making security a responsibility of everyone on the team. This article will walk you through how to help ensure your application is secure by adding continuous security validation to your CI/CD pipeline.  Security needs to shift from an afterthought to being evaluated at every step of the process. Securing applications is a continuous process that encompasses secure infrastructure, designing an architecture with layered security, continuous security validation, and monitoring for attacks. | Continuous security validation should be added at each step from development through production to help ensure the application is always secure. The goal of this approach is to switch the conversation with the security team from approving each release to approving the CI/CD process and having the ability to monitor and audit the process at any time. Depending on your platform and where your application is at in its lifecycle, you may need to consider implementing the tools gradually. Especially if your product is mature and you haven't previously run any security validation against your site or application.  Validation in the CI/CD begins before the developer commits his or her code. Static code analysis tools in the IDE provide the first line of defense to help ensure that security vulnerabilities are not introduced into the CI/CD process. The process for committing code into a central repository should have controls to help prevent security vulnerabilities from being introduced. Using Git source control in Azure DevOps with branch policies provides a gated commit experience that can provide this validation. By enabling branch policies on the shared branch, a pull request is required to initiate the merge process and ensure that all defined controls are being executed. The pull request should require a code review, which is the one manual but important check for identifying new issues being introduced into your code. Along with this manual check, commits should be linked to work items for auditing why the code change was made and require a continuous integration (CI) build process to succeed before the push can be completed.  The CI build should be executed as part of the pull request (PR-CI) process discussed above and once the merge is complete. Typically, the primary difference between the two runs is that the PR-CI process doesn't need to do any of the packaging/staging that is done in the CI build. These CI builds should run static code analysis tests to ensure that the code is following all rules for both maintenance and security. Several tools can be used for this.  Visual Studio Code Analysis and the Roslyn Security Analyzers  Checkmarx - A Static Application Security Testing (SAST) tool  BinSkim - A binary static analysis tool that provides security and correctness results for Windows portable executables  Other 3rd party tools | Learn how to add continuous security validation to your CI/CD pipeline  https://docs.microsoft.com/en-us/azure/devops/migrate/security-validation-cicd-pipeline?view=azure-devops |
|  |  | Each Development team follows their own set of rules to validate the applications security. |  |  |  |
|  |  | A set of security controls and validations are defined at organizational level, but is up to each development team to decide how to perform the validation |  |  |  |
|  |  | Every development team in the organization automate the Security Verification tests and integrate them as part of the dev ops workflows and release pipeline. |  |  |  |
| **SE03** | Is the Security Team using security information event management (SIEM) and security orchestration automated response (SOAR) solutions to get intelligent security analytics and threat intelligence across the enterprise? |  | An enterprise must have visibility into what's happening within their technical cloud estate. Security monitoring and audit logging of Azure platform services is a key component of a scalable framework.  Security Center helps you prevent, detect, and respond to threats, and provides you increased visibility into, and  control over, the security of your Azure resources. It provides integrated Security monitoring and policy  management across your Azure subscriptions, helps detect threats that might otherwise go unnoticed, and works  with a broad ecosystem of security solutions.  Azure Sentinel is your birds-eye view across the enterprise alleviating the stress of increasingly sophisticated attacks, increasing volumes of alerts, and long resolution time frames. | Implement Azure Security Center and Azure Sentinel for Security information and event management. | Azure Security Center documentation  https://docs.microsoft.com/en-us/azure/security-center/  Azure Sentinel documentation  https://docs.microsoft.com/en-us/azure/sentinel/  Azure security fundamentals documentation  https://docs.microsoft.com/en-us/azure/security/fundamentals/  Enterprise-scale security governance and compliance  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/security-governance-and-compliance |
|  |  | *No SIEM solution in place.* |  |  |  |
|  |  | A SIEM solution is implemented but is not centralizing and analyzing all the organization logs |  |  |  |
|  |  | we are using the new Azure Sentinel SIEM solution to centralize Cloud and On-Premises logs to collect, detect, investigate, and respond to incidents and suspicious activates at scale |  |  |  |
| **SE04** | (Skipped <update pending to official documents>) |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| **SE05** | What patch management solution are you using? |  | Patch Updates provide the basis for finding and fixing potential problems and simplify the software update  management process, both by reducing the number of software updates you must deploy in your enterprise and  by increasing your ability to monitor compliance. | Enable Azure Update Management for Windows and Linux VMs.  Monitor base operating system patching drift via Azure Monitor logs and Azure Security Center.  Define a process for emergency patching for critical vulnerabilities.  Define a process for patching for VMs that are offline for extended periods of time. | Update Management overview  https://docs.microsoft.com/en-us/azure/automation/update-management/update-mgmt-overview  Enterprise-scale security governance and compliance  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/security-governance-and-compliance |
|  |  | We do not have any systems Update Management solution |  |  |  |
|  |  | we use legacy, non-cloud-native update management solutions. |  |  |  |
|  |  | we use Azure Update Management solution to update their systems wherever they are |  |  |  |
| **SE06** | What is the current strategy for data encryption? (KM) |  | Encryption is a vital step toward ensuring data privacy, compliance, and data residency in Microsoft Azure. It's also one of the most important security concerns of many enterprises. This section covers design considerations and recommendations as they pertain to encryption and key management. | Default to Microsoft-managed keys for principal encryption functionality and use customer-managed keys when required.  Identify your requirements for using customer-managed keys for native encryption mechanisms such as Azure Storage encryption:  Customer-managed keys.  Whole-disk encryption for virtual machines (VMs).  Data-in-transit encryption.  Data-at-rest encryption.  Encryption of data at rest  Data at rest includes information that resides in persistent storage on physical media, in any digital format. The media can include files on magnetic or optical media, archived data, and data backups. Microsoft Azure offers a variety of data storage solutions to meet different needs, including file, disk, blob, and table storage. Microsoft also provides encryption to protect Azure SQL Database, Azure Cosmos DB, and Azure Data Lake.  Data encryption at rest is available for services across the software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) cloud models. This article summarizes and provides resources to help you use the Azure encryption options.  Azure disk encryption  You can protect Windows and Linux virtual machines by using Azure disk encryption, which uses Windows BitLocker technology and Linux DM-Crypt to protect both operating system disks and data disks with full volume encryption.  Encryption keys and secrets are safeguarded in your Azure Key Vault subscription. By using the Azure Backup service, you can back up and restore encrypted virtual machines (VMs) that use Key Encryption Key (KEK) configuration.  Encryption of data in transit  Azure offers many mechanisms for keeping data private as it moves from one location to another.  Data-link Layer encryption in Azure  Microsoft gives customers the ability to use Transport Layer Security (TLS) protocol to protect data when it’s traveling between the cloud services and customers. Microsoft datacenters negotiate a TLS connection with client systems that connect to Azure services. TLS provides strong authentication, message privacy, and integrity (enabling detection of message tampering, interception, and forgery), interoperability, algorithm flexibility, and ease of deployment and use.  Use a federated Azure Key Vault model to avoid transaction scale limits.  Provision Azure Key Vault with the soft delete and purge policies enabled to allow retention protection for deleted objects.  Follow a least privilege model by limiting authorization to permanently delete keys, secrets, and certificates to specialized custom Azure Active Directory (Azure AD) roles.  Automate the certificate management and renewal process with public certificate authorities to ease administration.  Establish an automated process for key and certificate rotation.  Enable firewall and virtual network service endpoint on the vault to control access to the key vault.  Use the platform-central Azure Monitor Log Analytics workspace to audit key, certificate, and secret usage within each instance of Key Vault.  Delegate Key Vault instantiation and privileged access and use Azure Policy to enforce a consistent compliant configuration.  Default to Microsoft-managed keys for principal encryption functionality and use customer-managed keys when required.  Don't use centralized instances of Key Vault for application keys or secrets.  Don't share Key Vault instances between applications to avoid secret sharing across environments. | Azure encryption overview  https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-overview  Enterprise-scale security governance and compliance  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/security-governance-and-compliance |
|  |  | We have not defined our Encryption requirements and policies yet |  |  |  |
|  |  | We have requirements for Encryption policies defined but not yet implemented / we use 3rd Party solutions to manage the Encryption of data uploaded to the Cloud (Client-side Encryption) |  |  |  |
|  |  | we leverage Key Vault for encryption, key, and certificate management |  |  |  |
| **CO01** | How are you handling data classification? |  | Organizations that are weak on data classification and file protection might be more susceptible to data leakage or data misuse. With proper file protection, you can analyze data flows to gain insight into your business, detect risky behaviors and take corrective measures, track access to documents, and so on.  You want to control and secure email, documents, and sensitive data that you share outside your company. Azure Information Protection is a cloud-based solution that helps an organization to classify, label, and protect its documents and emails. This can be done automatically by administrators who define rules and conditions, manually by users, or a combination where users get recommendations.  Classification is always identifiable, regardless of where the data is stored or with whom it’s shared. The labels include visual markings such as a header, footer, or watermark. Metadata is added to files and email headers in clear text. The clear text ensures that other services, such as solutions to prevent data loss, can identify the classification and take appropriate action.  The protection technology uses Azure Rights Management (Azure RMS). This technology is integrated with other Microsoft cloud services and applications, such as Microsoft 365 and Azure Active Directory. This protection technology uses encryption, identity, and authorization policies. Protection that is applied through Azure RMS stays with the documents and emails, independently of the location—inside or outside your organization, networks, file servers, and applications.  This information protection solution keeps you in control of your data, even when it’s shared with other people. You can also use Azure RMS with your own line-of-business applications and information protection solutions from software vendors, whether these applications and solutions are on-premises or in the cloud. | Deploy Azure Information Protection for your organization.  Apply labels that reflect your business requirements. For example: Apply a label named “highly confidential” to all documents and emails that contain top-secret data, to classify and protect this data. Then, only authorized users can access this data, with any restrictions that you specify.  Configure usage logging for Azure RMS so that you can monitor how your organization is using the protection service. | Azure data security and encryption best practices  https://docs.microsoft.com/en-us/azure/security/fundamentals/data-encryption-best-practices  Enterprise-scale security governance and compliance  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/security-governance-and-compliance |
|  |  | We do not have any data classification or labelling to categorize and protect their information |  |  |  |
|  |  | We have a data classification and protection in place for On-Prem documents, **and** **certain types of data** has **been** ported or migrated the solution to the Cloud |  |  |  |
|  |  | we are using Azure Information protection or similar solution to label and categorize their information based on confidentiality criteria |  |  |  |
| **SE08** | What is the key management strategy? |  | Subscription and scale limits as they apply to Azure Key Vault: Key Vault has transaction limits for keys and secrets. To throttle transactions per vault in a certain period, see Azure limits.  Key Vault serves a security boundary because access permissions for keys, secrets, and certificates are at the vault level. Key Vault access policy assignments grant permissions separately to keys, secrets, or certificates. They don't support granular, object-level permissions like a specific key, secret, or certificate key management.  You can isolate application-specific and workload-specific secrets and shared secrets, as appropriate control access.  You can optimize premium SKUs where hardware-security-module-protected keys are required. Underlying hardware security modules (HSMs) are FIPS 140-2 level 2 compliant. Manage Azure dedicated HSM for FIPS 140-2 level 3 compliance by considering the supported scenarios.  Key rotation and secret expiration.  Certificate procurement and signing by using Key Vault about certificates.  Alerting/notifications and automated certificate renewals.  Disaster recovery requirements for keys, certificates, and secrets.  Key Vault service replication and failover capabilities: availability and redundancy.  Monitoring key, certificate, and secret usage.  Detecting unauthorized access by using a key vault or Azure Monitor Log Analytics workspace: monitoring and alerting.  Delegated Key Vault instantiation and privileged access: secure access.  Requirements for using customer-managed keys for native encryption mechanisms such as Azure Storage encryption:  Customer-managed keys.  Whole-disk encryption for virtual machines (VMs).  Data-in-transit encryption.  Data-at-rest encryption. | Use a federated Azure Key Vault model to avoid transaction scale limits.  Provision Azure Key Vault with the soft delete and purge policies enabled to allow retention protection for deleted objects.  Follow a least privilege model by limiting authorization to permanently delete keys, secrets, and certificates to specialized custom Azure Active Directory (Azure AD) roles.  Automate the certificate management and renewal process with public certificate authorities to ease administration.  Establish an automated process for key and certificate rotation.  Enable firewall and virtual network service endpoint on the vault to control access to the key vault.  Use the platform-central Azure Monitor Log Analytics workspace to audit key, certificate, and secret usage within each instance of Key Vault.  Delegate Key Vault instantiation and privileged access and use Azure Policy to enforce a consistent compliant configuration.  Default to Microsoft-managed keys for principal encryption functionality and use customer-managed keys when required.  Don't use centralized instances of Key Vault for application keys or secrets.  Don't share Key Vault instances between applications to avoid secret sharing across environments.  Control who has access to Key Vaults and keys, grant access to users, groups, and applications at a specific scope.  Store certificates in your key vault. Your certificates are of high value. In the wrong hands, your application's security or the security of your data can be compromised.  Ensure that you can recover a deletion of key vaults or key vault objects. | Azure data security and encryption best practices  https://docs.microsoft.com/en-us/azure/security/fundamentals/data-encryption-best-practices  Enterprise-scale security governance and compliance  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/security-governance-and-compliance |
|  |  | we do not have a centralized key and secret management |  |  |  |
|  |  | we are using our own keys generated on On-premises hardware and is storing those keys on Azure Key Vault. However, there is a need to port this solution to a cloud native key management solution |  |  |  |
|  |  | we use Azure Key Vault as their cloud native key management solution and all the on-premises applications have access to the cloud management system |  |  |  |
| **CO02** | How are you handling data retention for audit data in Azure? |  | Be aware of data retention periods for audit data in Azure. For example, Azure AD Premium reports have a 30-day retention period by default.  Azure Activity Logs are kept in Azure Monitor for 90 days.  For most resources in Azure, metrics are stored for 93 days. There are some exceptions:  Guest OS Metrics:  Classic guest OS metrics. These are performance counters collected by the Windows Diagnostic Extension (WAD) or the Linux Diagnostic Extension (LAD) and routed to an Azure storage account. Retention for these metrics is 14 days.  Guest OS metrics sent to Azure Monitor Metrics. These are performance counters collected by the Windows Diagnostic Extension (WAD) and sent to the Azure Monitor data sink, or via the InfluxData Telegraf Agent on Linux machines. Retention for these metrics is 93 days.  Guest OS metrics collected by Log Analytics agent. These are performance counters collected by the Log Analytics agent and sent to a Log Analytics workspace. Retention for these metrics is 31 days and can be extended up to 2 years.  Application Insights log-based metrics:  Behind the scenes, log-based metrics translate into log queries. Their retention matches the retention of events in underlying logs. For Application Insights resources, logs are stored for 90 days.  You can enable long-term archiving of logs such as Azure activity logs, VM logs, and platform as a service (PaaS) logs in Azure. | Export Azure audit logs and Azure activity logs to Azure Monitor logs for long-term data retention. Export to Azure Storage for long-term storage beyond two years, if necessary. | Manage usage and costs with Azure Monitor Logs  https://docs.microsoft.com/en-us/azure/azure-monitor/platform/manage-cost-storage#change-the-data-retention-period  Metrics in Azure Monitor  https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-platform-metrics  Enterprise-scale security governance and compliance  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/security-governance-and-compliance |
|  |  | We do not have any data retention policies defined. |  |  |  |
|  |  | We have data retention / legal hold policies in place for On-Prem storage, but it has not been ported or migrated the solution to the Cloud |  |  |  |
|  |  | we are assigning data retention policies to storage services in the cloud |  |  |  |
| **CO03** | How are you handling regulatory and compliance requirements? |  | As business units request to deploy workloads to Azure, you need additional visibility into a workload to determine how to achieve appropriate levels of governance, security, and compliance. When a new service is required, you need to allow it.  Governance provides mechanisms and processes to maintain control over your applications and resources in Azure. Azure Policy is essential to ensuring security and compliance within enterprise technical estates. It can enforce vital management and security conventions across Azure platform services and supplement role-based access control (RBAC) that controls what actions authorized users can perform.  Microsoft Azure is the only cloud computing provider that offers a secure, consistent application platform and  infrastructure-as-a-service for teams to work within their different cloud skillsets and levels of project complexity,  with integrated data services and analytics that uncover intelligence from data wherever it exists, across both  Microsoft and non-Microsoft platforms, open frameworks and tools, providing choice for integrating cloud with on-premises  as well deploying Azure cloud services within on-premises datacenters. As part of the Microsoft Trusted  Cloud, customers rely on Azure for industry-leading security, reliability, compliance, privacy, and the vast network  of people, partners, and processes to support organizations in the cloud. | In Azure we design and manage the Azure infrastructure to meet a broad set of international and industry-specific  compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1, and SOC 2. We also meet country- or region specific  standards, including Australia IRAP, UK G-Cloud, and Singapore MTCS. Rigorous third-party audits, such  as those done by the British Standards Institute, verify adherence to the strict security controls these standards  mandate.  Determine what Azure policies are needed.  Enforce management and security conventions, such as the use of private endpoints.  Manage and create policy assignments by using policy definitions can be reused at multiple inherited assignment scopes. You can have centralized, baseline policy assignments at management group, subscription, and resource group scopes.  Ensure continuous compliance with compliance reporting and auditing.  Understand that Azure Policy has limits, such as the restriction of definitions at any particular scope: policy limits.  Understand regulatory compliance policies. These might include the health insurance portability and accountability act, payment card industry, data security standards, service organization controls trust service principals, and criteria.  Map regulatory and compliance requirements to Azure Policy definitions and Azure AD RBAC assignments.  Enable Security Center Standard for all subscriptions and use Azure Policy to ensure compliance. | Microsoft compliance offerings  https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-home?view=o365-worldwide  Azure security fundamentals documentation  https://docs.microsoft.com/en-us/azure/security/fundamentals/  Enterprise-scale security governance and compliance  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/security-governance-and-compliance |
|  |  | We do not have any regulatory and compliance policies **explicitly** defined and **documented.** |  |  |  |
|  |  | We have regulatory and compliance policies in place for On-Premises data, but it has not been ported or migrated the solution to the Cloud. |  |  |  |
|  |  | we have mapped regulatory and compliance requirements to Azure Policy definitions and Azure AD role-based access control assignments |  |  |  |
| **GO01** | Describe your approach to cloud governance. |  | The cloud creates new paradigms for the technologies that support the business. These new paradigms also change how those technologies are adopted, managed, and governed. When entire datacenters can be virtually torn down and rebuilt with one line of code executed by an unattended process, we have to rethink traditional approaches. This is especially true for governance.  Cloud governance is an iterative process. For organizations with existing policies that govern on-premises IT environments, cloud governance should complement those policies. The level of corporate policy integration between on-premises and the cloud varies depending on cloud governance maturity and a digital estate in the cloud. As the cloud estate changes over time, so do cloud governance processes and policies. The following exercises help you start building your initial governance foundation. | 1. Methodology: Establish a basic understanding of the methodology that drives cloud governance in the Cloud Adoption Framework to begin thinking through the end state solution.  2. Benchmark: Assess your current state and future state to establish a vision for applying the framework.  3. Initial governance foundation: Begin your governance journey with a small, easily implemented set of governance tools. This initial governance foundation is called a minimum viable product (MVP).  4. Improve the initial governance foundation: Throughout implementation of the cloud adoption plan, iteratively add governance controls to address tangible risks as you progress toward the end state.  Create Service Strategy document that contains at least:  Expected benefits and outcomes aligned with business objectives and how will you measure them  Cloud definition and workload placement criteria  Required roles and stakeholders  Completion criteria and Success Metrics  Workload assessment  Resourcing and budgeting  Architecture and Technical requirements  Risks, Assumptions and Dependencies  Adoption and Change Management approach  Identify required Azure tags and use the append policy mode to enforce usage.  Map regulatory and compliance requirements to Azure Policy definitions and Azure AD RBAC assignments.  Establish Azure Policy definitions at the top-level root management group so that they can be assigned at inherited scopes.  Manage policy assignments at the highest appropriate level with exclusions at bottom levels, if required.  Use Azure Policy to control resource provider registrations at the subscription and/or management group levels.  Use built-in policies where possible to minimize operational overhead.  Assign the built-in policy contributor role at a particular scope to enable application-level governance.  Limit the number of Azure Policy assignments made at the root management group scope to avoid managing through exclusions at inherited scopes. | Governance in the Microsoft Cloud Adoption Framework for Azure  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/govern/  Enterprise-scale security governance and compliance  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/security-governance-and-compliance |
|  |  | We have a dedicated Cloud migration team that consists of subject matter experts that have strong awareness of current technical estate. |  |  |  |
|  |  | We have an established structure with representation from Business, Finance, and IT to advocate, support and influence across the company. |  |  |  |
|  |  | We have a dedicated Cloud Strategy and Cloud Governance teams that consists of subject matter experts from Security, IT Ops, influencers from Finance, impacted Line of Business units, Architects and Business Decision Makers to assess business risks and tolerance levels. |  |  |  |
| **GO02** | Do you have a well- defined Resource Tagging and naming standards modelling? Do you enforce adherence to this modelling for new resources? |  | Changing resource names can be difficult. Establish a comprehensive naming convention before you begin any large cloud deployment.  A naming and tagging strategy includes business and operational details as components of resource names and metadata tags:  The business side of this strategy ensures that resource names and tags include the organizational information needed to identify the teams. Use a resource along with the business owners who are responsible for resource costs.  The operational side ensures that names and tags include information that IT teams use to identify the workload, application, environment, criticality, and other information useful for managing resources.  An effective naming convention assembles resource names by using important resource information as parts of a resource's name. For example, using these recommended naming conventions, a public IP resource for a production SharePoint workload is named like this: pip-sharepoint-prod-westus-001.  From the name, you can quickly identify the resource's type, its associated workload, its deployment environment, and the Azure region hosting it.  When you apply metadata tags to your cloud resources, you can include information about those assets that couldn't be included in the resource name. You can use that information to perform more sophisticated filtering and reporting on resources. You want these tags to include context about the resource's associated workload or application, operational requirements, and ownership information. This information can be used by IT or business teams to find resources or generate reports about resource usage and billing. | Identify required Azure tags and use the append policy mode to enforce usage.  Define naming standards for Azure resources for your organization.  Use Azure Policy to enforce naming and tagging to Azure resources  Be aware that some resource names, such as PaaS services with public endpoints or virtual machine DNS labels, have global scopes, which means that they must be unique across the entire Azure platform.  When you construct your naming convention, identify the key pieces of information that you want to reflect in a resource name. Different information is relevant for different resource types. The following list provides examples of information that are useful when you construct resource names. | Recommended naming and tagging conventions  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/naming-and-tagging  Enterprise-scale security governance and compliance  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/security-governance-and-compliance |
|  |  | we are not using Tags and does not have Naming Standards definition |  |  |  |
|  |  | We have Naming Standards definition and use tags for some resources. Resource tagging is not being enforced by Azure Policies |  |  |  |
|  |  | We have a Naming Standards, and all the Resources are using Tags based on Business, Departments, Application or billing requirements. Tags are being enforced through Azure Policies and. |  |  |  |
| **GO03** | What is your platform security strategy in Azure? |  | You must maintain a healthy security posture as you adopt Azure. Besides visibility, you have to be able to control the initial settings and changes as the Azure services evolve. Therefore, planning for platform security is key. | In the context of your underlying requirements, conduct a joint examination of each required service. If you want to bring your own keys, this might not be supported across all considered services. Implement relevant mitigation so that inconsistencies don't hinder desired outcomes. Choose appropriate region pairs and disaster recovery regions that minimize latency.  Develop a security allow-list plan to assess services security configuration, monitoring, alerts, and how to integrate these with existing systems.  Determine the incident response plan for Azure services before allowing.  Use Azure AD reporting capabilities to generate access control audit reports.  Align your security requirements with Azure platform roadmaps to stay current with newly released security controls.  Implement a zero-trust approach for access to the Azure platform, where appropriate. | Enterprise-scale security governance and compliance  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/security-governance-and-compliance |
|  |  | We do not have a cloud strategy and security requirements defined yet. |  |  |  |
|  |  | we have a set of Azure policies defined to, but they are assigned manually when new resources are being deployed. |  |  |  |
|  |  | we have a well-defined set of policies and requirements. We have a cloud strategy team to define and mandate security across our cloud environment. |  |  |  |
| **GO04** | Do you have a well-defined role-based access to manage keys, certificates, and secrets in your cloud environment? |  | Azure Key Vault is a cloud service that safeguards encryption keys and secrets like certificates, connection strings, and passwords. Because this data is sensitive and business critical, you need to secure access to your key vaults by allowing only authorized applications and users. This article provides an overview of the Key Vault access model. It explains authentication and authorization and describes how to secure access to your key vaults.  Key Vault serves a security boundary because access permissions for keys, secrets, and certificates are at the vault level. Key Vault access policy assignments grant permissions separately to keys, secrets, or certificates. They don't support granular, object-level permissions like a specific key, secret, or certificate key management.  If a user has Contributor permissions to a key vault management plane, the user can grant themselves access to the data plane by setting a Key Vault access policy. You should tightly control who has Contributor role access to your key vaults. Ensure that only authorized persons can access and manage your key vaults, keys, secrets, and certificates. | Follow a least privilege model by limiting authorization to permanently delete keys, secrets, and certificates to specialized custom Azure Active Directory (Azure AD) roles.  Delegate Key Vault instantiation and privileged access and use Azure Policy to enforce a consistent compliant configuration.  Use the platform-central Azure Monitor Log Analytics workspace to audit key, certificate, and secret usage within each instance of Key Vault.  You can create a key vault in a resource group and manage access by using Azure AD. You grant users or groups the ability to manage the key vaults in a resource group. You grant the access at a specific scope level by assigning appropriate Azure roles. To grant access to a user to manage key vaults, you assign a predefined key vault Contributor role to the user at a specific scope. The following scopes levels can be assigned to an Azure role:  Subscription: An Azure role assigned at the subscription level applies to all resource groups and resources within that subscription.  Resource group: An Azure role assigned at the resource group level applies to all resources in that resource group.  Specific resource: An Azure role assigned for a specific resource applies to that resource. In this case, the resource is a specific key vault.  There are several predefined roles. If a predefined role doesn't fit your needs, you can define your own role.  Enable Monitoring key, certificate, and secret usage to detect unauthorized access by using a key vault or Azure Monitor Log Analytics workspace. | Secure access to a key vault  https://docs.microsoft.com/en-us/azure/key-vault/general/secure-your-key-vault  Azure built-in roles  https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles  Enterprise-scale security governance and compliance  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/security-governance-and-compliance |
|  |  | Not being defined/ used. Every administrator in the organization is either Owner or Contributor. |  |  |  |
|  |  | We are using common built-in RBAC roles from Azure roles. Access is not being monitored. |  |  |  |
|  |  | We are using RBAC and Time-bound Access through Azure AD Privileged Identity Management (PIM) for managing and monitoring access reviews. |  |  |  |
| **GO05** | Do you have a Cost Management strategy and a solution in place? |  | Cost management is the process of effectively planning and controlling costs involved in your business. Cost management tasks are typically performed by finance, management, and app teams. Azure Cost Management and Billing can help you plan with cost in mind. It can also help you to analyze costs effectively and take action to optimize cloud spending. | If the organization already has a cloud strategy in place, ensure the inclusion of cost management strategies. Else define a cost management strategy that includes and is built on the understanding of investment returns, operational efficiencies, and value propositions.  Evaluate your Cost Management toolchain options.  Develop a draft document for architecture guidelines and distribute to key stakeholders.  Educate and involve the people and teams affected by the development of architecture guidelines.  Ensure budgetary decisions that support the business justification for your cloud strategy.  Validate learning metrics that you use to report on the successful allocation of funding.  Understand the desired cloud accounting model that affects how cloud costs should be accounted for.  Become familiar with the digital estate plan and validate accurate costing expectations.  Evaluate buying options to determine whether it's better to ""pay as you go"" or to make a precommitment by purchasing an Enterprise Agreement.  Align business goals with planned budgets and adjust budgetary plans as necessary.  Develop a goals and budget reporting mechanism to notify technical and business stakeholders at the end of each cost cycle. | Get started: Manage cloud costs  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/get-started/manage-costs  Cost Management discipline improvement  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/govern/cost-management/discipline-improvement  Azure Cost Management + Billing documentation  https://docs.microsoft.com/en-us/azure/cost-management-billing/ |
|  |  | we do not have any product, automation, or Dashboard to control Azure Spending. Most of the Cost Management is done manually on daily, weekly, and monthly basis by checking the portal information. |  |  |  |
|  |  | we use a small subset of capabilities listed above but can improve their Azure spending by implementing more automation on deeper monitoring. |  |  |  |
|  |  | We have a cloud accounting model, for Show Back, Charge Back, Awareness Back, or Central IT cost structures. We have processes for allocating cost accordingly. |  |  |  |

* 1. Additional findings and Recommendations

1. Platform Automation and DevOps
   1. Assessment details

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Label | Question | Answer | Why consider this | Suggested Actions | Learn More |
| **DO01** | Do you currently have a centralized DevOps team in the organization? |  | Many traditional IT operating models aren't compatible with the cloud, and organizations must undergo operational and organizational transformation to deliver against enterprise migration targets. You should use a DevOps approach for both application and central teams. | Establish a cross-functional DevOps platform team to build, manage, and maintain your enterprise-scale architecture. This team should include members from your central IT team, security, compliance, and business units to ensure that a wide spectrum of your enterprise is represented. | Platform automation and DevOps  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/platform-automation-and-devops |
|  |  | We are following **Application CI/CD,** but we do not have a cross functional DevOps Platform Team. |  |  |  |
|  |  | We have established a DevOps team, but we do not have members from business unit/security team. |  |  |  |
|  |  | We have established a **cross functional DevOps Platform Team** to build, manage and maintain your Enterprise Scale architecture. This team includes members from our central IT, security, compliance, and business units’ teams to ensure a wide spectrum of your enterprise is represented. Central teams strive to maintain full control whilst application owners seek to maximize agility. The balance between these goals can greatly influence the success of the migration |  |  |  |
| **DO02** | Do you have a clear definition of roles and responsibilities for your DevOps teams? |  | Investing in engineering capabilities and resources is critical.  You can arrange internal and external DevOps roles and functions from a variety of sources that align with your organization's strategy.  For some legacy apps, the associated app team might not have engineering resources required to align with a DevOps strategy. | Establish a cross-functional DevOps platform team to build, manage, and maintain your enterprise-scale architecture. This team should include members from your central IT team, security, compliance, and business units to ensure that a wide spectrum of your enterprise is represented. The following list presents a recommended set of DevOps roles for a central platform team:  PlatformOps (platform operations) for:  Subscription provisioning and delegation of required network, identity and access management, and policies.  Platform management and monitoring (holistic).  Cost management (holistic).  Platform-as-code (managing templates, scripts, and other assets).  Responsible for overall operations on Microsoft Azure within the Azure Active Directory tenant (managing service principals, Graph API registration, and defining roles).  SecOps (security operations)  Role-based access control (RBAC) (holistic).  Key management (for central services, simple mail-transfer protocol, and domain controller).  Policy management and enforcement (holistic).  Security monitoring and audit (holistic).  NetOps (network operations)  Network management (holistic).  AppDevOps. Allow app owners to create and manage app resources through a DevOps model. The following list presents a recommended DevOps role for application teams:  App migration or transformation.  App management and monitoring.  RBAC (app resources).  Security monitoring and audit (app resources).  Cost management (app resources).  Network management (app resources).  In some instances, you might want to break AppDevOps into more granular roles such as AppDataOps for database management or AppSecOps for more security-sensitive apps.  Provide a central app DevOps function to support apps that don't have existing DevOps capabilities or a business case to establish one (for example, legacy apps with minimal development capabilities).  Use RBAC. RBAC allows organizations to assign different teams to various management tasks within large cloud estates. It can allow Central IT teams to control core access and security features, while also giving software developers and other teams large amounts of control over specific workloads or groups of resources.  Most cloud environments can also benefit from an access-control strategy that uses multiple roles and emphasizes a separation of responsibilities between these roles. This approach requires that any significant change to resources or infrastructure involves multiple roles to complete, ensuring that more than one person must review and approve a change. This separation of responsibilities limits the ability of a single person to access sensitive data or introduce vulnerabilities without the knowledge of other team members. | Platform automation and DevOps  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/platform-automation-and-devops  Role-based access control  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/considerations/roles |
|  |  | We use our on-premises traditional identity and access management model to Azure resources and services. |  |  |  |
|  |  | We have established some **roles** in Azure as **Applications** and Central **Functions**, but there is still a gap to fill all requirements for managing cloud applications and resources. |  |  |  |
|  |  | "We have **clear definitions of roles for Applications Functions and Central Functions**, striving to empower migration/transformation activities with minimal central dependencies while still supporting the centralized governance of security and operability across the entire estate |  |  |  |
| **DO03** | Is assigning RBAC and Policies part of the application release process? |  | To accelerate Azure adoption, the central platform team should establish a common set of templates and libraries for application teams to draw upon. For example, horizontal (cross-function) guidance can help to support migrations through subject matter expertise and to ensure alignment with the overall target enterprise-scale architecture. | Use a policy-driven approach with clear RBAC boundaries to centrally enforce consistency and security across application teams. This ensures a least privilege approach is taken by using a combination of RBAC assignments and Azure Policy, and that workloads are always compliant with Azure Policy assignments  Don't restrict application teams to use central artifacts or approaches because it hinders their agility. You can enforce consistent baseline configurations through a policy-driven infrastructure approach and RBAC assignments. This ensures that app (business unit) teams are flexible enough to innovate while still able to draw from a predefined set of templates.  Don't force application teams to use a central process or provisioning pipeline for the instantiation or management of app resources. Existing teams that already rely on a DevOps pipeline for app delivery should still be able to use the same tools they have been using. Remember that you can still use Azure Policy to maintain guard rails, independent of how resources are deployed in Azure. | Platform automation and DevOps  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/platform-automation-and-devops |
|  |  | Our platform team creates a relevant resource so apps team can deploy and release their applications in Azure. |  |  |  |
|  |  | Resources are created automatically as part of release. **Azure Policies and RBAC** are assigned manually after the resources are deployed. |  |  |  |
|  |  | We use a **policy-driven approach with clear RBAC boundaries** to centrally enforce consistency and security across application teams. This ensures a least privilege approach is taken by **using a combination of RBAC assignments and Azure Policy**, and that workloads are always compliant with Azure Policy assignments. |  |  |  |
| **CP01** | How agile, do you consider, is the development process? |  | Central teams strive to maintain full control while app owners seek to maximize agility. The balance between these goals can greatly influence the success of the migration. | Don't restrict application teams to use central artifacts or approaches because it hinders their agility. You can enforce consistent baseline configurations through a policy-driven infrastructure approach and RBAC assignments. This ensures that app (business unit) teams are flexible enough to innovate while still able to draw from a predefined set of templates. | Platform automation and DevOps  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/platform-automation-and-devops |
|  |  | Not very, we must stick to our roadmap |  |  |  |
|  |  | Fair, we need a couple of sprints to change direction |  |  |  |
|  |  | Very, we can change according to changed priority almost instantly |  |  |  |
| **CI01** | What files do you keep under source control? |  | A source control system, also called a version control system, allows developers to collaborate on code and track changes. Source control is an essential tool for multi-developer projects.  If Azure DevOps used, our systems support two types of source control: Git (distributed) and Team Foundation Version Control (TFVC). TFVC is a centralized, client-server system. In both Git and TFVC, you can check in files and organize files in folders, branches, and repositories.  Git is a popular distributed version control system. When you use Git for source control, you have a complete copy of the repository with all of its history on your local computer. Many people prefer that because it's easier to continue working when you're not connected to the network -- you can continue to do commits and rollbacks, create and switch branches, and so forth. Even when you're connected to the network, it's easier and quicker to create branches and switch branches when everything is local. You can also do local commits and rollbacks without having an impact on other developers. And you can batch commits before sending them to the server.  With Git, each developer has a copy of the source repository on their dev machine. The source repo includes all branch and history information. Each developer works directly with their local repository. Changes are shared between repositories as a separate step.  Developers can commit each set of changes and perform version control operations, such as history and compare without a network connection. Branches are lightweight. When developers need to switch contexts, they create a private local branch. Developers can quickly switch from one branch to another to pivot among different variations of the code base. Later, developers can merge, publish, or dispose of the branch.  With TFVC, developers have only one version of each file on their dev machines. Historical data is maintained only on the server. Branches are path-based and are created on the server. | Use any source control environment to implement the DevOps branching structure for your applications and infrastructure. Using a distributed version control system (DVCS).  The master branch always matches code that is in production. Branches underneath master correspond to different stages in the development life cycle. The development branch is where you implement new features. For a small team you might just have master and development, but we often recommend that people have a staging branch between development and master. You can use staging for final integration testing before an update is moved to production.  For big teams there may be separate branches for each new feature; for a smaller team you might have everyone checking in to the development branch.  If you have a branch for each feature, when Feature A is ready you merge its source code changes up into the development branch and down into the other feature branches. This source code merging process can be time-consuming, and to avoid that work while still keeping features separate, some teams implement an alternative called feature toggles (also known as feature flags). This means all of the code for all of the features is in the same branch, but you enable or disable each feature by using switches in the code. For example, suppose Feature A is a new field for Fix It app tasks, and Feature B adds caching functionality. The code for both features can be in the development branch, but the app will only display the new field when a variable is set to true, and it will only use caching when a different variable is set to true. If Feature A isn't ready to be promoted but the Feature B is ready, you can promote all of the code to Production with the Feature A switch off and the Feature B switch on. You can then finish Feature A and promote it later, all with no source code merging.  Whether or not you use branches or toggles for features, a branching structure like this enables you to flow your code from development into production in an agile and repeatable way.  This structure also enables you to react quickly to customer feedback. If you need to make a quick fix to production, you can also do that efficiently in an agile way. You can create a branch off of master or staging, and when it's ready merge it up into master and down into development and feature branches.  Infrastructure as Code (IaC) is the management of infrastructure (networks, virtual machines, load balancers, and connection topology) in a descriptive model, using the same versioning as DevOps team uses for source code. Like the principle that the same source code generates the same binary, an IaC model generates the same environment every time it is applied. IaC is a key DevOps practice and is used in conjunction with continuous delivery.  Infrastructure as Code evolved to solve the problem of environment drift in the release pipeline. Without IaC, teams must maintain the settings of individual deployment environments. Over time, each environment becomes a snowflake, that is, a unique configuration that cannot be reproduced automatically. Inconsistency among environments leads to issues during deployments. With snowflakes, administration and maintenance of infrastructure involves manual processes which were hard to track and contributed to errors.  Your Azure landing zones environments for hosting your workloads should be pre provisioned through code. Since landing zone infrastructure is defined in code, it can be refactored similar to any other codebase. Refactoring is the process of modifying or restructuring source code to optimize the output of that code without changing its purpose or core function. | What is source control?  https://docs.microsoft.com/en-us/azure/devops/user-guide/source-control?view=azure-devops  Source Control (Building Real-World Cloud Apps with Azure)  https://docs.microsoft.com/en-us/aspnet/aspnet/overview/developing-apps-with-windows-azure/building-real-world-cloud-apps-with-windows-azure/source-control |
|  |  | **Application** source code |  |  |  |
|  |  | Application source code, **tests, and configuration files** |  |  |  |
|  |  | All files used to build, test, configure, deploy, run, and document our service. |  |  |  |
| **CI02** | What is your branching policy? |  | Distributed version control systems like Git give you flexibility in how you use version control to share and manage code. Your team should find a balance between this flexibility and the need to collaborate and share code in a consistent manner.  Team members publish, share, review, and iterate on code changes through Git branches shared with others. Adopt a branching strategy for your team. You can collaborate better and spend less time managing version control and more time developing code. | Develop your features and fix bugs in feature branches based off your main branch. These branches are also known as topic branches. Feature branches isolate work in progress from the completed work in the main branch. Git branches are inexpensive to create and maintain. Even small fixes and changes should have their own feature branch.  The code in your main branch should pass tests, build cleanly, and always be current. Your main branch needs these qualities so that feature branches created by your team start from a known good version of code.  Set up a branch policy for your main branch that:  Requires a pull request to merge code. This approach prevents direct pushes to the main branch and ensures discussion of proposed changes.  Automatically adds reviewers when a pull request is created. The added team members review the code and comment on the changes in the pull request.  Requires a successful build to complete a pull request. Code merged into the main branch should build cleanly.  Setup branch policies to help teams protect your important branches of development. Policies enforce your team's code quality and change management standards. | Adopt a Git branching strategy  https://docs.microsoft.com/en-us/azure/devops/repos/git/git-branching-guidance?view=azure-devops  Improve code quality with branch policies  https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-policies?view=azure-devops  Microsoft Branching Strategy (example)  https://docs.microsoft.com/en-us/azure/devops/learn/devops-at-microsoft/release-flow  " |
|  |  | We keep new work in separate branches and merge only when finished, usually in weeks or months |  |  |  |
|  |  | We use branches that live for a few days max and commit all changes to the master or trunk at least daily |  |  |  |
|  |  | We keep traceability on code changes but treat branches as temporary by using topic branches that we squash-merge to master when the work is complete |  |  |  |
| **CI03** | How do you manage code dependencies across teams? |  | Distributed version control systems like Git give you flexibility in how you use version control to share and manage code. Your team should find a balance between this flexibility and the need to collaborate and share code in a consistent manner.  Team members publish, share, review, and iterate on code changes through Git branches shared with others. Adopt a branching strategy for your team. You can collaborate better and spend less time managing version control and more time developing code. | Use a distributed source control system so DevOps team has copy of the code on their dev machine from the source repository, including all branch and history information. Each developer works directly with their own local repository and changes are shared between repositories as a separate step.  Share code as binary assets and track control dependencies.  You can use Azure DevOps Boards or GitHub Issues and Projects. | Azure Boards documentation  https://docs.microsoft.com/en-us/azure/devops/boards/?view=azure-devops  Azure Artifacts documentation  https://docs.microsoft.com/en-us/azure/devops/artifacts/?view=azure-devops |
|  |  | We track them in a **spreadsheet,** or document / We use a work item tracking system. |  |  |  |
|  |  | The dependencies are **published as packages to a repository**, so we can track the dependencies in our code. We publish our own artifacts as well so other teams that depend on us can see the new artifacts. |  |  |  |
|  |  | We have a full open-source model, so anyone can contribute and use our code as well as we can use other teams code |  |  |  |
| **CD01** | How does your product get deployed and released? |  | Implementing CI and CD pipelines helps to ensure consistent and quality code that's readily available to users. And Azure Pipelines provides a quick, easy, and safe way to automate building your projects and making them available to users.  Use Azure Pipelines because it supports the following scenarios:  Works with any language or platform  Deploys to different types of targets at the same time  Integrates with Azure deployments  Builds on Windows, Linux, or Mac machines  Integrates with GitHub  Works with open-source projects. | If using Azure DevOps: Use Azure DevOps Pipelines when working with continuous deployment to promote builds from your main branch to your deployment targets.  Where central teams are concerned, you should use pipelines for continuous integration and continuous deployment. Use the pipelines to manage policy definitions, role definitions, policy assignments, management group hierarchies, and subscriptions. These pipelines help ensure that you can operationally manage multiple subscriptions while still conforming to a desired state.  If using GitHub: Use GitHub Actions to help you automate tasks within your software development life cycle. GitHub Actions are event-driven, meaning that you can run a series of commands after a specified event has occurred. For example, every time someone creates a pull request for a repository, you can automatically run a command that executes a software testing script." | Azure Pipelines documentation  https://docs.microsoft.com/en-us/azure/devops/pipelines/?view=azure-devops  Platform automation and DevOps  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/platform-automation-and-devops  GitHub Actions  https://docs.github.com/en/actions |
|  |  | Manual deployments to all environments. |  |  |  |
|  |  | Continuous deployment to Production / A combination of Manual and Automated Steps |  |  |  |
|  |  | Continuous deployment to staging environment(s) and gated deployment to Production |  |  |  |
| **CQ01** | What is your team's standard for testing? |  | Quality is a vital aspect of software systems, and manual testing and exploratory testing continue to be an important techniques for maximizing this.  Manual testing has evolved with the software development process into a more agile-based approach. Azure DevOps and TFS integrate manual testing into your agile processes; the team can begin manual testing right from their Kanban boards in the Work hub. Teams that need more advanced capabilities can use the Test hub for all their test management needs.  In today's software development processes and infrastructure as code, everybody in the team owns quality - including developers, managers, product owners, user experience advocates, and more. | Use Azure Test Plans feature which provides tooling to develop and operate test plans for manual or automated test executions. | Azure Test Plans documentation  https://docs.microsoft.com/en-us/azure/devops/test/?view=azure-devops |
|  |  | Testing that validates conformance to **requirements** and fixes of identified **bugs** |  |  |  |
|  |  | Testing that covers most used **functionality, data, code paths and configurations**, with coverage measured against them |  |  |  |
|  |  | Testing that promotes continuous improvement in user satisfaction, quality of service, and performance on business objectives |  |  |  |
| **CS01** | What security practices does your team apply to the system you are developing? |  | Development and operations are tightly integrated to enable fast and continuous delivery of value to end users. DevOps has replaced siloed development and operations to create multidisciplinary teams that work together with shared and efficient practices, tools, and KPIs. To deliver highly secure software and services in this fast-moving environment, it is critical for security to move at the same speed. One way to achieve this is to build security in development (SDL) and operations (OSA) processes. | Provide Training  Establish a minimum-security baseline that takes account of both security and compliance controls. Ensure these are baked into the DevOps process and pipeline. At the very minimum, ensure the baseline considers real-world threats such as the OWASP Top 10 or SANS Top 25, and industry or regulatory requirements and issues known to exist or that could be introduced by human error in the technology stack you select.  Define Metrics and Compliance Reporting  Use Software Composition Analysis (SCA) and Governance  Perform Threat Modeling  Use Tools and Automation  Keep Credentials Safe  Continuous Learning and Monitoring | Secure DevOps  https://www.microsoft.com/en-us/securityengineering/devsecops |
|  |  | Secure coding **practices** |  |  |  |
|  |  | **Static** Code security and vulnerability scanning |  |  |  |
|  |  | **Dynamic** Code security and vulnerability scanning |  |  |  |
| **CO01** | How do development and operations teams collaborate during a production issue? |  | Many traditional IT operating models aren't compatible with the cloud, and organizations must undergo operational and organizational transformation to deliver against enterprise migration targets. You should use a DevOps approach for both application and central teams. | Dev and Ops teams must improve collaboration in order to improve efficiency, reduce troubleshooting times, and reduce errors introduced between life-cycle stages. Even the smallest configuration error can result in long delays, requiring both Dev and Ops teams to identify and resolve problems, ultimately extending release times.  DevOps teams must seek to identify issues before they affect the customer experience and mitigate issues quickly when they do occur. Maintaining this vigilance requires rich telemetry, actionable alerting and full visibility into applications and the underlying system. | What is DevOps?  https://azure.microsoft.com/en-ca/overview/what-is-devops/ |
|  |  | Production incidents are handled by **operations** staff. Only If all operational procedures have failed to restore service level, then an escalation process may be started on an exception basis to engage developers. |  |  |  |
|  |  | They **collaborate in real time**, in a physical team room/war room or online chat room, IRC, IM, or other messaging channel |  |  |  |
|  |  | Devs and Ops do a **joint** retrospective to review the root cause of an issue once it's resolved. They plan how to prevent a recurrence. |  |  |  |
| **CC01** | How does your team collaborate, share risks, innovate, and learn? |  | Continuous Collaboration encourages you to value:  Individuals and interactions over processes and tools  Working software over comprehensive documentation  Customer collaboration over contract negotiation  Responding to change over following a plan | Continuous Collaboration is a practice that supports the cultural shifts that are key to any DevOps journey. Continuous Collaboration enables teams to innovate outside of the boundaries of planned meetings and fosters innovation within the team by creating an integrated experience.  Silos can be broken down using technologies and practices that make it possible for teams to work together even if no ideal co-location exists.  Review The Agile Manifesto from the perspective of Continuous Collaboration and you will realize that it really is all about the value of collaborating and having personal interactions in order to truly innovate | What is DevOps?  https://azure.microsoft.com/en-ca/overview/what-is-devops/  Characterize DevOps Continuous Collaboration and Continuous Improvement  https://docs.microsoft.com/en-us/learn/modules/characterize-devops-continous-collaboration-improvement/ |
|  |  | There is some **communication**. When mistakes are made, there is justice for the responsible person |  |  |  |
|  |  | Communication and collaboration is good among teams. Innovation is encouraged. |  |  |  |
|  |  | There is **high cooperation among teams**. Risks are shared. Failure leads to learning and inquiry to help the team improve. Innovation is encouraged and implemented |  |  |  |
| **CU01** | Can you feel the organization moving to applying a more agile approach? |  | The rules have changed, and organizations around the world are now adapting their approach to software development accordingly. Agile methods and practices don’t promise to solve every problem. But they do promise to establish a culture and environment where solutions emerge… through collaboration, continual planning and learning, and a desire to ship high quality software more often.  Agile is a term used to describe approaches to software development emphasizing incremental delivery, team collaboration, continual planning, and continual learning. The term “Agile” was coined in 2001 in the Agile Manifesto. The manifesto set out to establish principles to guide a better approach to software development. | Deploy applications and infrastructure using an automated pipeline and  DevOps. The full automation of all steps between code commit to production deployment allows teams to focus on building code and removes the overhead and potential  human error in manual mundane steps. Deploying new code is quicker and less risky, helping teams become more agile, more productive, and more confident about their running code.  Provide DevOps and agile methodologies training opportunities to the team.  When the team culture isn't ready for agile processes, you might find innovation and keeping pace with the market to be a challenge. | What is Agile?  https://docs.microsoft.com/en-us/azure/devops/learn/agile/what-is-agile  For training resources about DevOps and agile practices:  Evolve your DevOps practices  https://docs.microsoft.com/en-us/learn/paths/evolve-your-devops-practices/  Build applications with Azure DevOps  https://docs.microsoft.com/en-us/learn/paths/build-applications-with-azure-devops/ |
|  |  | No, it's hard to introduce agile practices / No, we don't even consider this. |  |  |  |
|  |  | Yes, but our organization has a long some way to go |  |  |  |
|  |  | Yes, we already are agile and are improving every sprint |  |  |  |
| **CD02** | How do you roll out new features to users? |  | Continuous Delivery (CD) is the process to build, test, configure and deploy from a build to a production environment. Multiple testing or staging environments create a Release Pipeline to automate the creation of infrastructure and deployment of a new build. Successive environments support progressively longer-running activities of integration, load, and user acceptance testing. Continuous Integration starts the CD process, and the pipeline stages each successive environment to the next upon successful completion of tests.  Continuous Delivery may sequence multiple deployment “rings” for progressive exposure (also known as “controlling the blast radius”). Progressive exposure groups users who get to try new releases to monitor their experience in “rings.” The first deployment ring is often a “canary” used to test new versions in production before a broader rollout. CD automates deployment from one ring to the next and may optionally depend on an approval step, in which a decision maker signs off on the changes electronically. CD may create an auditable record of the approval in order to satisfy regulatory procedures or other control objectives.  Without Continuous Delivery, software release cycles were previously a bottleneck for application and operation teams. Manual processes led to unreliable releases that produced delays and errors. These teams often relied on handoffs that resulted in issues during release cycles. The automated release pipeline allows a “fail fast” approach to validation, where the tests most likely to fail quickly are run first and longer-running tests happen after the faster ones complete successfully. | Continuously delivering value has become a mandatory requirement for organizations. To deliver value to your end users, you must release continually and without errors. | What is Continuous Delivery?  https://docs.microsoft.com/en-us/azure/devops/learn/what-is-continuous-delivery  Platform automation and DevOps  https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/platform-automation-and-devops |
|  |  | We deploy when the appropriate manager approves |  |  |  |
|  |  | We run a full test suite in a **production-realistic environment** and then deploy |  |  |  |
|  |  | We use progressive deployment with feature flags or exposure control and watch telemetry to determine whether to continue rollout |  |  |  |

* 1. Additional findings and Recommendations

1. Next steps and Recommended Engagements

[Short paragraph to describe what next steps actions and recommended engagements are required before customer can get into CAF Landing Zone Design Workshop]

Example:

|  |  |
| --- | --- |
| **Design Area** | **Need to Take foundational services to get ready for CAF Landing Zone** |
| Identity and access management | **Architectural Service - Azure Active Directory: Designing a Secure Cloud Identity** |
| Network topology and connectivity | **Activate Azure with Hybrid Cloud**  **Activate Azure with Enterprise-grade Networking** |
| Management and monitoring | **WorkshopPLUS - Azure Modern Monitoring and Management or Activate Azure with Azure Monitor**  **Modern Service Management Foundations for Azure** |
| Security, governance, and compliance | **WorkshopPLUS - Microsoft Azure: Security Best Practices**  **Security: Azure Security Center – Fundamentals**  **Activate Azure with Administration and Governance** |
| Platform automation and DevOps | **WorkshopPLUS Azure Infrastructure as Code**  **WorkshopPLUS - Azure DevOps Services: Essentials** |