Regulatory Compliance and Remediation Plan

# 1. Storage Accounts Compliance

|  |  |  |  |
| --- | --- | --- | --- |
| **Finding** | **Terraform Action** | **Remediation Action** | **Azure Policy Available?** |
| 3.1: Ensure ‘Secure transfer required’ is set to ‘Enabled’ | Set `secure\_transfer\_enabled = true` in `azurerm\_storage\_account`. | Enable secure transfer for all storage accounts. | Yes - 'Secure transfer should be enabled' |
| 3.2: Enable Infrastructure Encryption | Use `infrastructure\_encryption\_enabled = true` in `azurerm\_storage\_account`. | Enable infrastructure encryption for additional security. | Yes - 'Enable infrastructure encryption for storage' |
| 3.3: Enable Key Rotation Reminders | Use `azurerm\_key\_vault\_key` with a rotation policy. | Set up key rotation reminders in Azure Key Vault. | No (Custom Policy recommended) |
| 3.4: Periodic Regeneration of Storage Account Access Keys | Use Azure Automation or Key Vault for periodic key rotation scripts. | Schedule access key regeneration through automation. | No (Custom Policy recommended) |
| 3.5: Enable Storage Logging for Queue Service | Configure `azurerm\_monitor\_diagnostic\_setting` for queue service logging. | Enable logging for queue services on ‘Read’, ‘Write’, ‘Delete’. | Yes - 'Enable diagnostics logs for storage services' |
| 3.6: SAS Token Expiration within an Hour | Use policy to enforce SAS token expiry in storage account settings. | Review and enforce SAS token expiry to one hour max. | Yes - 'Enforce SAS token expiration time' |
| 3.7: Disable Public Access Level for Blob Containers | Set `allow\_blob\_public\_access = false` in `azurerm\_storage\_account`. | Set blob container public access level to private. | Yes - 'Disable public blob access' |
| 3.8: Set Default Network Access Rule to ‘Deny’ | Use `default\_action = Deny` in `azurerm\_storage\_account\_network\_rules`. | Restrict access by setting default network access rule to 'Deny'. | Yes - 'Set default network access to Deny' |
| 3.9: Allow Azure Services Access on Trusted Services List | Configure trusted services access in `azurerm\_storage\_account\_network\_rules`. | Enable trusted services list access to storage accounts. | Yes - 'Allow trusted services access to storage' |
| 3.10: Use Private Endpoints for Storage Accounts | Use `azurerm\_private\_endpoint` to connect storage accounts privately. | Implement private endpoints to restrict access. | Yes - 'Enforce private endpoints for storage accounts' |
| 3.11: Enable Soft Delete for Blob Storage | Set `soft\_delete\_retention\_days` in `azurerm\_storage\_account`. | Enable Soft Delete for blob data protection. | Yes - 'Enable soft delete for blobs' |
| 3.12: Encrypt Critical Data with Customer-Managed Keys (CMKs) | Use `azurerm\_storage\_account` with CMK configuration. | Enable CMK encryption for storage of critical data. | Yes - 'Encrypt storage with CMKs' |
| 3.13: Enable Storage Logging for Blob Service | Configure `azurerm\_monitor\_diagnostic\_setting` for Blob logging. | Enable blob logging for ‘Read’, ‘Write’, ‘Delete’ requests. | Yes - 'Enable diagnostics logs for storage services' |
| 3.14: Enable Storage Logging for Table Service | Configure `azurerm\_monitor\_diagnostic\_setting` for Table service logging. | Enable table logging for ‘Read’, ‘Write’, ‘Delete’ operations. | Yes - 'Enable diagnostics logs for storage services' |
| 3.15: Set Minimum TLS Version to 1.2 | Set `min\_tls\_version = "TLS1\_2"` in `azurerm\_storage\_account`. | Configure storage accounts to use TLS version 1.2. | Yes - 'Enforce TLS 1.2 or higher' |

# 2. Virtual Machines Compliance

|  |  |  |  |
| --- | --- | --- | --- |
| **Finding** | **Terraform Action** | **Remediation Action** | **Azure Policy Available?** |
| 7.1: Ensure an Azure Bastion Host Exists | Deploy `azurerm\_bastion\_host`. | Set up an Azure Bastion Host for secure access. | No (Custom Policy recommended) |
| 7.2: Ensure Virtual Machines are utilizing Managed Disks | Ensure VMs use `azurerm\_managed\_disk`. | Migrate to managed disks for all VMs. | Yes - 'Enforce managed disks' |
| 7.3: Ensure that ‘OS and Data’ disks are encrypted with CMK | Use `disk\_encryption\_set\_id` with `azurerm\_managed\_disk`. | Enable CMK encryption on VM disks. | Yes - 'Disks should be encrypted with CMK' |
| 7.4: Ensure that ‘Unattached disks’ are encrypted with CMK | Use `azurerm\_disk\_encryption\_set`. | Ensure unattached disks are encrypted with CMK. | Yes - 'Unattached disks should be encrypted' |
| 7.5: Ensure that Only Approved Extensions Are Installed | Use allowed `azurerm\_virtual\_machine\_extension`. | Audit and remove unapproved extensions. | Yes - 'Only approved VM extensions should be installed' |
| 7.6: Ensure that Endpoint Protection for all VMs is Installed | Use `azurerm\_security\_center\_contact` to enable endpoint protection. | Enable endpoint protection via Security Center. | Yes - 'Endpoint protection should be enabled' |
| 7.7: [Legacy] Ensure that VHDs are Encrypted | Use `azurerm\_disk\_encryption\_set` to apply encryption to VHDs. | Encrypt legacy VHDs. | No (Custom Policy recommended) |

# 3. Identity and Access Management

|  |  |  |  |
| --- | --- | --- | --- |
| **Finding** | **Terraform Action** | **Remediation Action** | **Azure Policy Available?** |
| 1.1: Security Defaults | Configure security defaults in Azure AD settings. | Enable security defaults for enhanced protection. | Yes - 'Enable security defaults' |
| 1.2: Conditional Access | Define conditional access policies in Azure AD. | Enforce conditional access across the organization. | Yes - 'Enforce conditional access policies' |
| 1.3: Ensure that ‘Users can create Azure AD tenants’ is set to ‘No’ | Configure Azure AD tenant settings to restrict creation. | Restrict users from creating Azure AD tenants. | Yes - 'Restrict Azure AD tenant creation' |
| 1.4: Set Up Access Review for External Users | Use Azure AD PIM to configure access reviews. | Set up periodic access reviews for external users. | Yes - 'Require access review for external users' |
| 1.5: Ensure Guest Users Are Reviewed Regularly | Configure Azure AD PIM access review policies. | Implement access reviews for guest users regularly. | Yes - 'Enforce guest user access review' |

# 4. Database Services Compliance

|  |  |  |  |
| --- | --- | --- | --- |
| **Finding** | **Terraform Action** | **Remediation Action** | **Azure Policy Available?** |
| 4.1.1: Ensure that ‘Auditing’ is set to ‘On’ | Use `azurerm\_sql\_server` with `extended\_auditing\_policy`. | Enable SQL auditing to monitor database activities. | Yes - 'Enable SQL auditing' |
| 4.1.2: Restrict Azure SQL Database Ingress from 0.0.0.0 | Use `azurerm\_sql\_firewall\_rule` to restrict ingress IPs. | Prevent incoming connections from 0.0.0.0 on SQL databases. | Yes - 'Restrict ingress IP for SQL databases' |
| 4.1.3: Enable CMK for TDE | Use `azurerm\_key\_vault\_key` with `transparent\_data\_encryption`. | Enable TDE with CMK for SQL Server encryption. | Yes - 'Enable CMK for TDE' |
| 4.1.4: Configure Azure AD Admin for SQL Server | Use `administrator\_login` in `azurerm\_sql\_server` to configure AD. | Set up Azure AD admin for SQL Servers. | Yes - 'Configure SQL servers with AAD admin' |
| 4.1.5: Enable Data Encryption on SQL Database | Use `transparent\_data\_encryption\_enabled` in `azurerm\_sql\_database`. | Enable data encryption on SQL databases for security. | Yes - 'Enable data encryption on SQL databases' |
| 4.1.6: Extend SQL Auditing Retention to 90+ Days | Set `retention\_in\_days` in SQL auditing policy. | Configure audit retention to retain logs for over 90 days. | Yes - 'Enforce auditing retention policy' |

# 5. App Service Compliance

|  |  |  |  |
| --- | --- | --- | --- |
| **Finding** | **Terraform Action** | **Remediation Action** | **Azure Policy Available?** |
| 9.1: Ensure App Service Authentication is set up | Use `identity` block with `azurerm\_app\_service`. | Enable AAD authentication for App Services. | Yes - 'App Service should have AAD authentication' |
| 9.2: Redirect HTTP to HTTPS | Configure `https\_only` in `azurerm\_app\_service`. | Enforce HTTPS redirection on web apps. | Yes - 'Enforce HTTPS redirection' |
| 9.3: Use Latest TLS Version | Set `min\_tls\_version` to `1.2` or higher in `azurerm\_app\_service`. | Enable latest TLS version for App Services. | Yes - 'Enforce TLS version 1.2 or higher' |
| 9.4: Enable Client Certificates | Enable `client\_cert\_enabled` in `azurerm\_app\_service`. | Require client certificates for web app access. | Yes - 'Require client certificates for App Services' |
| 9.5: Register with Azure AD | Configure AAD settings in `azurerm\_app\_service`. | Enable AAD registration for App Services. | Yes - 'Register App Service with AAD' |
| 9.6: Ensure Latest PHP Version | Use `php\_version` in `azurerm\_app\_service` configuration. | Update to the latest stable PHP version. | Yes - 'Ensure latest PHP version' |
| 9.7: Ensure Latest Python Version | Use `python\_version` in `azurerm\_app\_service` configuration. | Update to the latest stable Python version. | Yes - 'Ensure latest Python version' |
| 9.8: Ensure Latest Java Version | Use `java\_version` in `azurerm\_app\_service` configuration. | Update to the latest stable Java version. | Yes - 'Ensure latest Java version' |
| 9.9: Ensure Latest HTTP Version | Configure `http\_version` to `2.0` in `azurerm\_app\_service`. | Ensure HTTP version 2.0 or higher is used. | Yes - 'Ensure HTTP version 2.0 or higher' |
| 9.10: Disable FTP Deployments | Set `ftps\_state` to `Disabled` in `azurerm\_app\_service`. | Disable FTP for improved security. | Yes - 'Disable FTP access for App Services' |
| 9.11: Use Azure Key Vault for Secrets | Use `azurerm\_key\_vault\_secret` to manage secrets securely. | Store secrets in Azure Key Vault instead of app config. | Yes - 'Enforce Key Vault for secrets storage' |

# 6. Role Definitions and Multi-Factor Authentication

|  |  |  |  |
| --- | --- | --- | --- |
| **Finding** | **Terraform Action** | **Remediation Action** | **Azure Policy Available?** |
| 1.18: Restrict Access to Groups Features in Access Panel | Configure Azure AD settings in `azurerm\_role\_definition`. | Limit users' access to groups in the Access Panel. | Yes - 'Restrict user access in Access Panel' |
| 1.19: Disable Security Group Creation by Users | Use Azure AD `group\_settings` to limit group creation. | Restrict group creation in portals, API, and PowerShell. | Yes - 'Restrict security group creation' |
| 1.20: Restrict Group Membership Management by Owners | Set permissions in Azure AD group settings. | Prevent owners from managing group membership requests. | Yes - 'Restrict group membership requests management' |
| 1.21: Restrict Microsoft 365 Group Creation | Configure group creation restrictions in Azure AD settings. | Limit Microsoft 365 group creation permissions. | Yes - 'Restrict Microsoft 365 group creation' |
| 1.22: Enforce Multi-Factor Authentication (MFA) | Configure MFA for devices in Azure AD settings. | Enable MFA for registering and joining devices. | Yes - 'Require MFA for device registration' |
| 1.23: No Custom Subscription Admin Roles | Use `azurerm\_role\_definition` to audit and remove custom roles. | Remove custom subscription administrator roles. | Yes - 'Restrict custom subscription admin roles' |

# 7. Access Control & Virtual Machines

|  |  |  |  |
| --- | --- | --- | --- |
| **Finding** | **Terraform Action** | **Remediation Action** | **Azure Policy Available?** |
| A9.1: Access control policy | Define RBAC roles and permissions in `azurerm\_role\_assignment`. | Review and enforce access control policies. | Yes - 'Access control policies' |
| A9.1.2: Access to networks and network services | Implement managed identity using `azurerm\_user\_assigned\_identity` for access. | Enable managed identity and Guest Configuration. | No (Custom Policy recommended) |
| - Add system-assigned managed identity to enable Guest Configuration assignment | Configure `identity` block in VM resources to enable system identity. | Add system-assigned managed identities to VMs. | Yes - 'Enable managed identities for VMs' |
| - Audit Linux machines that have accounts without passwords | Use Guest Configuration policy for auditing. | Enable audit for Linux machines without passwords. | Yes - 'Audit Linux machines with accounts without passwords' |
| - Deploy the Linux Guest Configuration extension | Use `azurerm\_virtual\_machine\_extension` for Linux Guest Configuration. | Deploy Guest Configuration extension to Linux VMs. | Yes - 'Linux Guest Configuration extension' |
| - Audit VMs that do not use managed disks | Use policy to ensure VMs are on managed disks. | Audit and migrate unmanaged disks to managed disks. | Yes - 'Ensure VMs use managed disks' |