Azure Cloud Audit Checklist

SACHIN HISSARIA
CA | CISA | DISA | CEH | COBIT-19 | ISO27001:2022 |CC - (ISC2)| RPA | Trainer

Sr. No	Control	Risk	Auditors Remarks
1	**Ensure 'HTTPS Only' is set to `On` (Automated)** Azure App Service allows apps to run under both HTTP and HTTPS by default. Apps can be accessed by anyone using non-secure HTTP links by default. Non-secure HTTP requests can be restricted and all HTTP requests redirected to the secure HTTPS port. It is recommended to enforce HTTPS-only traffic.	Enabling HTTPS-only traffic will redirect all non-secure HTTP requests to HTTPS ports. HTTPS uses the TLS/SSL protocol to provide a secure connection which is both encrypted and authenticated. It is therefore important to support HTTPS for the security benefits.	
2	**Ensure App Service Authentication is set up for apps in Azure App Service (Automated)** Azure App Service Authentication is a feature that can prevent anonymous HTTP requests from reaching a Web Application or authenticate those with tokens before they reach the app. If an anonymous request is received from a browser, App Service will redirect to a logon page. To handle the logon process, a choice from a set of identity providers can be made, or a custom authentication mechanism can be implemented.	By Enabling App Service Authentication, every incoming HTTP request passes through it before being handled by the application code. It also handles authentication of users with the specified provider (Azure Active Directory, Facebook, Google, Microsoft Account, and Twitter), validation, storing and refreshing of tokens, managing the authenticated sessions and injecting identity information into request headers.	
3	**Ensure 'FTP State' is set to 'FTPS Only' or 'Disabled' (Automated)** By default, App Services can be deployed over FTP. If FTP is required for an essential deployment workflow, FTPS should be required for FTP login for all App Services. If FTPS is not expressly required for the App, the recommended setting is Disabled.	FTP is an unencrypted network protocol that will transmit data - including passwords - in clear-text. The use of this protocol can lead to both data and credential compromise, and can present opportunities for exfiltration, persistence, and lateral movement.	
4	**Ensure Web App is using the latest version of TLS encryption (Automated)** The TLS (Transport Layer Security) protocol secures transmission of data over the internet using standard encryption technology. Encryption should be set with the latest version of TLS. App service allows TLS 1.2 by default, which is the recommended TLS level by industry standards such as PCI DSS.	App service currently allows the web app to set TLS versions 1.0, 1.1 and 1.2. It is highly recommended to use the latest TLS 1.2 version for web app secure connections.	
5	**Ensure the web app has 'Client Certificates (Incoming client certificates)' set to 'On' (Automated)** Client certificates allow for the app to request a certificate for incoming requests. Only clients that have a valid certificate will be able to reach the app.	The TLS mutual authentication technique in enterprise environments ensures the authenticity of clients to the server. If incoming client certificates are enabled, then only an authenticated client who has valid certificates can access the app.	
6	**Ensure that Register with Azure Active Directory is enabled on App Service (Automated)** Managed service identity in App Service provides more security by eliminating secrets from the app, such as credentials in the connection strings. When registering with Azure Active Directory in App Service, the app will connect to other Azure services securely without the need for usernames and passwords.	App Service provides a highly scalable, self-patching web hosting service in Azure. It also provides a managed identity for apps, which is a turn-key solution for securing access to Azure SQL Database and other Azure services.	
7	**Ensure that 'PHP version' is currently supported (if in use) (Manual)** Periodically, older versions of PHP may be deprecated and no longer supported. Using a supported version of PHP for web apps is recommended to avoid potential unpatched vulnerabilities.	Deprecated and unsupported versions of programming and scripting languages can present vulnerabilities which may not be addressed or may not be addressable.	
8	**Ensure that 'Python version' is currently supported (if in use) (Manual)** Periodically, older versions of Python may be deprecated and no longer supported. Using a supported version of Python for web apps is recommended to avoid potential unpatched vulnerabilities.	Deprecated and unsupported versions of programming and scripting languages can present vulnerabilities which may not be addressed or may not be addressable.	
9	**Ensure that 'Java version' is currently supported (if in use) (Manual)** Periodically, older versions of Java may be deprecated and no longer supported. Using a supported version of Java for web apps is recommended to avoid potential unpatched vulnerabilities.	Deprecated and unsupported versions of programming and scripting languages can present vulnerabilities which may not be addressed or may not be addressable.	

Sr. No	Control	Risk	Auditors Remarks
10	**Ensure that 'HTTP20enabled' is set to 'true' (if in use) (Automated)** Periodically, older versions of HTTP may be deprecated and no longer supported. Using a supported version of HTTP for web apps is recommended to avoid vulnerabilities from outdated protocols. HTTP 2.0 has additional performance improvements on the head-of-line blocking problem of old HTTP version, header compression, and prioritization of requests. HTTP 2.0 no longer supports HTTP 1.1's chunked transfer encoding mechanism, as it provides its own, more efficient, mechanisms for data streaming.	Deprecated and unsupported versions of protocols such as HTTP can present vulnerabilities which may not be addressed or may not be addressable.	
11	**Ensure Azure Key Vaults are Used to Store Secrets (Manual)** Azure Key Vault will store multiple types of sensitive information such as encryption keys, certificate thumbprints, and Managed Identity Credentials. Access to these 'Secrets' can be controlled through granular permissions.	The credentials given to an application have permissions to create, delete, or modify data stored within the systems they access. If these credentials are stored within the application itself, anyone with access to the application or a copy of the code has access to them. Storing within Azure Key Vault as secrets increases security by controlling access. This also allows for updates of the credentials without redeploying the entire application.	
12	**Ensure Private Virtual Networks are used for Container Instances (Manual)** Private Virtual Networks (vNets) ensure that services and hosts within the subscription environment are appropriately segmented in private subnets. Public IP addressing for container instances should be handled through a NAT gateway and/or Firewall. In addition to the use of a private vNet for container instances, ensure that a Network Security Group (NSG) is configured and applied to your container instance vNet. The NSG will need to be configured with inbound and outbound TCP/UDP traffic rules which reflect the needs of the services running in your container instance.	Network segmentation reduces threat surface and limits potential lateral movement in the case of breach. Container instances with Public IP addresses present significant threat surface and should be avoided.	
13	**Ensure Private Virtual Networks are used for Container Instances (Manual)** Private Virtual Networks (vNets) ensure that services and hosts within the subscription environment are appropriately segmented in private subnets. Public IP addressing for container instances should be handled through a NAT gateway and/or Firewall. In addition to the use of a private vNet for container instances, ensure that a Network Security Group (NSG) is configured and applied to your container instance vNet. The NSG will need to be configured with inbound and outbound TCP/UDP traffic rules which reflect the needs of the services running in your container instance.	Network segmentation reduces threat surface and limits potential lateral movement in the case of breach. Container instances with Public IP addresses present significant threat surface and should be avoided.	
14	**Ensure a Managed Identity is used for interactions with other Azure services (Manual)** For containers that require access to other resources, or other resources accessing a container, an identity/credential may be required. The Managed Identity prevents needing to store credentials in code within the Container Instance. There are two types of Managed Identities for Container Instances: 1.System Assigned: System Assigned Managed Identities provide an infrastructure integrated identity which is unique to the resource. It assigned to the Container Instance and persists for the lifecycle of the resource. Permissions can be assigned, revoked, and tuned using Azure role-based access control. 2.User Assigned: User Assigned Managed Identities are not unique to the resource, and exist as independent Azure resources with their own lifecycle. If a Container Identity is decommissioned, the User Assigned Managed Identity will need to be decommissioned	Identities or credentials stored within a Container Instance or the code running on the Container Instance introduce a risk of compromise. If that identity or credential is stored in plain text, the risk is further amplified.	
15	**Ensure the principle of least privilege is used when assigning roles to a Managed Identity (Manual)** When using either a user-assigned or system-assigned managed identity, those identities may require a role or privilege assignment to perform a desired function. The roles or privileges assigned to that identity should be assigned with the principle of least privilege in mind - the identity is given the minimum levels of access or permissions needed to perform the job.	Threat actors may attempt to compromise service accounts as anomalous activity on these accounts can sometimes be more challenging to detect. Limiting the permissions or roles available to a managed identity or service account assists in mitigating the systemic exploitation that a service account can perform if compromised.	

Sr. No	Control	Risk	Auditors Remarks
16	**Ensure SSL is configured for CycleCloud (Manual)** The use of SSL ensures that data in transit to and from the Azure CycleCloud server is encrypted.	Encryption of data in transit provides integrity and confidentiality to that data. If unencrypted data is intercepted in transit it is highly vulnerable to exposure and exploitation.	
17	**Ensure an Azure Bastion Host Exists (Automated)** The Azure Bastion service allows secure remote access to Azure Virtual Machines over the Internet without exposing remote access protocol ports and services directly to the Internet. The Azure Bastion service provides this access using TLS over 443/TCP, and subscribes to hardened configurations within an organization's Azure Active Directory service.	The Azure Bastion service allows organizations a more secure means of accessing Azure Virtual Machines over the Internet without assigning public IP addresses to those Virtual Machines. The Azure Bastion service provides Remote Desktop Protocol (RDP) and Secure Shell (SSH) access to Virtual Machines using TLS within a web browser, thus preventing organizations from opening up 3389/TCP and 22/TCP to the Internet on Azure Virtual Machines. Additional benefits of the Bastion service includes Multi-Factor Authentication, Conditional Access Policies, and any other hardening measures configured within Azure Active Directory using a central point of access.	
18	**Ensure Virtual Machines are utilizing Managed Disks (Automated)** Migrate blob-based VHDs to Managed Disks on Virtual Machines to exploit the default features of this configuration. The features include: 1.Default Disk Encryption 2.Resilience, as Microsoft will managed the disk storage and move around if underlying hardware goes faulty 3.Reduction of costs over storage accounts	Managed disks are by default encrypted on the underlying hardware, so no additional encryption is required for basic protection. It is available if additional encryption is required. Managed disks are by design more resilient that storage accounts. For ARM-deployed Virtual Machines, Azure Adviser will at some point recommend moving VHDs to managed disks both from a security and cost management perspective.	
19	**Ensure that 'OS and Data' disks are encrypted with Customer Managed Key (CMK) (Automated)** Ensure that OS disks (boot volumes) and data disks (non-boot volumes) are encrypted with CMK (Customer Managed Keys). Customer Managed keys can be either ADE or Server Side Encryption (SSE).	Encrypting the IaaS VM's OS disk (boot volume) and Data disks (non-boot volume) ensures that the entire content is fully unrecoverable without a key, thus protecting the volume from unwanted reads. PMK (Platform Managed Keys) are enabled by default in Azure-managed disks and allow encryption at rest. CMK is recommended because it gives the customer the option to control which specific keys are used for the encryption and decryption of the disk. The customer can then change keys and increase security by disabling them instead of relying on the PMK key that remains unchanging. There is also the option to increase security further by using automatically rotating keys so that access to disk is ensured to be limited. Organizations should evaluate what their security requirements are, however, for the data stored on the disk. For high-risk data using CMK is a must, as it provides extra steps of security. If the data is low risk, PMK is enabled by default and provides	
20	**Ensure that 'Unattached disks' are encrypted with 'Customer Managed Key' (CMK) (Automated)** Ensure that unattached disks in a subscription are encrypted with a Customer Managed Key (CMK).	Managed disks are encrypted by default with Platform-managed keys. Using Customer-managed keys may provide an additional level of security or meet an organization's regulatory requirements. Encrypting managed disks ensures that its entire content is fully unrecoverable without a key and thus protects the volume from unwarranted reads. Even if the disk is not attached to any of the VMs, there is always a risk where a compromised user account with administrative access to VM service can mount/attach these data disks, which may lead to sensitive information disclosure and tampering.	

Sr. No	Control	Risk	Auditors Remarks
21	**Ensure that Only Approved Extensions Are Installed (Manual)** For added security, only install organization-approved extensions on VMs.	Azure virtual machine extensions are small applications that provide post-deployment configuration and automation tasks on Azure virtual machines. These extensions run with administrative privileges and could potentially access anything on a virtual machine. The Azure Portal and community provide several such extensions. Each organization should carefully evaluate these extensions and ensure that only those that are approved for use are actually implemented.	
22	**Ensure that Endpoint Protection for all Virtual Machines is installed (Manual)** Install endpoint protection for all virtual machines.	Installing endpoint protection systems (like anti-malware for Azure) provides for real-time protection capability that helps identify and remove viruses, spyware, and other malicious software. These also offer configurable alerts when known-malicious or unwanted software attempts to install itself or run on Azure systems.	
23	**[Legacy] Ensure that VHDs are Encrypted (Manual)** NOTE: This is a legacy recommendation. Managed Disks are encrypted by default and recommended for all new VM implementations. VHD (Virtual Hard Disks) are stored in blob storage and are the old-style disks that were attached to Virtual Machines. The blob VHD was then leased to the VM. By default, storage accounts are not encrypted, and Microsoft Defender will then recommend that the OS disks should be encrypted. Storage accounts can be encrypted as a whole using PMK or CMK. This should be turned on for storage accounts containing VHDs.	While it is recommended to use Managed Disks which are encrypted by default, "legacy" VHDs may exist for a variety of reasons and may need to remain in VHD format. VHDs are not encrypted by default, so this recommendation intends to address the security of these disks. In these niche cases, VHDs should be encrypted using the procedures in this recommendation to encrypt and protect the data content. If a virtual machine is using a VHD and can be converted to a managed disk, instructions for this procedure can be found in the resources section of this recommendation under the title "Convert VHD to Managed Disk."	