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 the Storage Container Storing the Activity Logs is not Publicly Accessible (Automated)** The storage account container containing the activity log export should not be publicly accessible.	Allowing public access to activity log content may aid an adversary in identifying weaknesses in the affected account's use or configuration.	
2	**Ensure the storage account containing the container with activity logs is encrypted with Customer Managed Key (Automated)** Storage accounts with the activity log exports can be configured to use Customer Managed Keys (CMK).	Configuring the storage account with the activity log export container to use CMKs provides additional confidentiality controls on log data, as a given user must have read permission on the corresponding storage account and must be granted decrypt permission by the CMK.	
3	**Ensure that logging for Azure Key Vault is 'Enabled' (Automated)** Enable AuditEvent logging for key vault instances to ensure interactions with key vaults are logged and available.	Monitoring how and when key vaults are accessed, and by whom, enables an audit trail of interactions with confidential information, keys, and certificates managed by Azure Keyvault. Enabling logging for Key Vault saves information in an Azure storage account which the user provides. This creates a new container named insights-logs-auditevent automatically for the specified storage account. This same storage account can be used for collecting logs for multiple key vaults.	
4	**Ensure that Network Security Group Flow logs are captured and sent to Log Analytics (Manual)** Ensure that network flow logs are captured and fed into a central log analytics workspace.	Network Flow Logs provide valuable insight into the flow of traffic around your network and feed into both Azure Monitor and Azure Sentinel (if in use), permitting the generation of visual flow diagrams to aid with analyzing for lateral movement, etc.	
5	**Ensure that logging for Azure AppService 'HTTP logs' is enabled (Manual)** Enable AppServiceHTTPLogs diagnostic log category for Azure App Service instances to ensure all http requests are captured and centrally logged.	Capturing web requests can be important supporting information for security analysts performing monitoring and incident response activities. Once logging, these logs can be ingested into SIEM or other central aggregation point for the organization.	
6	**Ensure that Activity Log Alert exists for Create Policy Assignment (Automated)** Create an activity log alert for the Create Policy Assignment event.	Monitoring for create policy assignment events gives insight into changes done in "Azure policy - assignments" and can reduce the time it takes to detect unsolicited changes.	
7	**Ensure that Activity Log Alert exists for Delete Policy Assignment (Automated)** Create an activity log alert for the Delete Policy Assignment event.	Monitoring for delete policy assignment events gives insight into changes done in "azure policy - assignments" and can reduce the time it takes to detect unsolicited changes.	
8	**Ensure that Activity Log Alert exists for Create or Update Network Security Group (Automated)** Create an Activity Log Alert for the Create or Update Network Security Group event.	Monitoring for Create or Update Network Security Group events gives insight into network access changes and may reduce the time it takes to detect suspicious activity.	
9	**Ensure that Activity Log Alert exists for Delete Network Security Group (Automated)** Create an activity log alert for the Delete Network Security Group event.	Monitoring for "Delete Network Security Group" events gives insight into network access changes and may reduce the time it takes to detect suspicious activity.	
10	**Ensure that Activity Log Alert exists for Create or Update Security Solution (Automated)** Create an activity log alert for the Create or Update Security Solution event.	Monitoring for Create or Update Security Solution events gives insight into changes to the active security solutions and may reduce the time it takes to detect suspicious activity.	
11	**Ensure that Activity Log Alert exists for Delete Security Solution (Automated)** Create an activity log alert for the Delete Security Solution event.	Monitoring for Delete Security Solution events gives insight into changes to the active security solutions and may reduce the time it takes to detect suspicious activity.	
12	**Ensure that Activity Log Alert exists for Create or Update SQL Server Firewall Rule (Automated)** Create an activity log alert for the Create or Update SQL Server Firewall Rule event.	Monitoring for Create or Update SQL Server Firewall Rule events gives insight into network access changes and may reduce the time it takes to detect suspicious activity.	
13	**Ensure that Activity Log Alert exists for Delete SQL Server Firewall Rule (Automated)** Create an activity log alert for the "Delete SQL Server Firewall Rule."	Monitoring for Delete SQL Server Firewall Rule events gives insight into SQL network access changes and may reduce the time it takes to detect suspicious activity.	

Sr. No	Control	Risk	Auditors Remarks
14	**Ensure that Activity Log Alert exists for Create or Update Public IP Address rule (Automated)** Create an activity log alert for the Create or Update Public IP Addresses rule.	Monitoring for Create or Update Public IP Address events gives insight into network access changes and may reduce the time it takes to detect suspicious activity.	
15	**Ensure that Activity Log Alert exists for Delete Public IP Address rule (Automated)** Create an activity log alert for the Delete Public IP Address rule.	Monitoring for Delete Public IP Address events gives insight into network access changes and may reduce the time it takes to detect suspicious activity.	
16	**Ensure Application Insights are Configured (Automated)** Application Insights within Azure act as an Application Performance Monitoring solution providing valuable data into how well an application performs and additional information when performing incident response. The types of log data collected include application metrics, telemetry data, and application trace logging data providing organizations with detailed information about application activity and application transactions. Both data sets help organizations adopt a proactive and retroactive means to handle security and performance related metrics within their modern applications.	Configuring Application Insights provides additional data not found elsewhere within Azure as part of a much larger logging and monitoring program within an organization's Information Security practice. The types and contents of these logs will act as both a potential cost saving measure (application performance) and a means to potentially confirm the source of a potential incident (trace logging). Metrics and Telemetry data provide organizations with a proactive approach to cost savings by monitoring an application's performance, while the trace logging data provides necessary details in a reactive incident response scenario by helping organizations identify the potential source of an incident within their application.	
17	**Ensure that Azure Monitor Resource Logging is Enabled for All Services that Support it (Manual)** Resource Logs capture activity to the data access plane while the Activity log is a subscription-level log for the control plane. Resource-level diagnostic logs provide insight into operations that were performed within that resource itself; for example, reading or updating a secret from a Key Vault. Currently, 95 Azure resources support Azure Monitoring (See the more information section for a complete list), including Network Security Groups, Load Balancers, Key Vault, AD, Logic Apps, and CosmosDB. The content of these logs varies by resource type. A number of back-end services were not configured to log and store Resource Logs for certain activities or for a sufficient length. It is crucial that monitoring is correctly configured to log all relevant activities and retain those logs for a sufficient length of time. Given that the mean time to detection in an enterprise is 240 days, a minimum retention period of two years is recommended.	A lack of monitoring reduces the visibility into the data plane, and therefore an organization's ability to detect reconnaissance, authorization attempts or other malicious activity. Unlike Activity Logs, Resource Logs are not enabled by default. Specifically, without monitoring it would be impossible to tell which entities had accessed a data store that was breached. In addition, alerts for failed attempts to access APIs for Web Services or Databases are only possible when logging is enabled.	
18	**Ensure that SKU Basic/Consumption is not used on artifacts that need to be monitored (Particularly for Production Workloads) (Automated)** The use of Basic or Free SKUs in Azure whilst cost effective have significant limitations in terms of what can be monitored and what support can be realized from Microsoft. Typically, these SKU's do not have a service SLA and Microsoft will usually refuse to provide support for them. Consequently Basic/Free SKUs should never be used for production workloads.	Typically, production workloads need to be monitored and should have an SLA with Microsoft, using Basic SKUs for any deployed product will mean that that these capabilities do not exist. The following resource types should use standard SKUs as a minimum. • Public IP Addresses • Network Load Balancers • REDIS Cache • SQL PaaS Databases • VPN Gateways	
19	**Ensure that RDP access from the Internet is evaluated and restricted (Automated)** Network security groups should be periodically evaluated for port misconfigurations. Where certain ports and protocols may be exposed to the Internet, they should be evaluated for necessity and restricted wherever they are not explicitly required.	The potential security problem with using RDP over the Internet is that attackers can use various brute force techniques to gain access to Azure Virtual Machines. Once the attackers gain access, they can use a virtual machine as a launch point for compromising other machines on an Azure Virtual Network or even attack networked devices outside of Azure.	
20	**Ensure that SSH access from the Internet is evaluated and restricted (Automated)** Network security groups should be periodically evaluated for port misconfigurations. Where certain ports and protocols may be exposed to the Internet, they should be evaluated for necessity and restricted wherever they are not explicitly required.	The potential security problem with using SSH over the Internet is that attackers can use various brute force techniques to gain access to Azure Virtual Machines. Once the attackers gain access, they can use a virtual machine as a launch point for compromising other machines on the Azure Virtual Network or even attack networked devices outside of Azure.	

Sr. No	Control	Risk	Auditors Remarks
21	**Ensure that UDP access from the Internet is evaluated and restricted (Automated)** Network security groups should be periodically evaluated for port misconfigurations. Where certain ports and protocols may be exposed to the Internet, they should be evaluated for necessity and restricted wherever they are not explicitly required.	The potential security problem with broadly exposing UDP services over the Internet is that attackers can use DDoS amplification techniques to reflect spoofed UDP traffic from Azure Virtual Machines. The most common types of these attacks use exposed DNS, NTP, SSDP, SNMP, CLDAP and other UDP-based services as amplification sources for disrupting services of other machines on the Azure Virtual Network or even attack networked devices outside of Azure.	
22	**Ensure that HTTP(S) access from the Internet is evaluated and restricted (Automated)** Network security groups should be periodically evaluated for port misconfigurations. Where certain ports and protocols may be exposed to the Internet, they should be evaluated for necessity and restricted wherever they are not explicitly required and narrowly configured.	The potential security problem with using HTTP(S) over the Internet is that attackers can use various brute force techniques to gain access to Azure resources. Once the attackers gain access, they can use the resource as a launch point for compromising other resources within the Azure tenant.	
23	**Ensure that Network Security Group Flow Log retention period is 'greater than 90 days' (Automated)** Network Security Group Flow Logs should be enabled and the retention period set to greater than or equal to 90 days.	Flow logs enable capturing information about IP traffic flowing in and out of network security groups. Logs can be used to check for anomalies and give insight into suspected breaches.	
24	**Ensure that Network Watcher is 'Enabled' (Automated)** Enable Network Watcher for Azure subscriptions.	Network diagnostic and visualization tools available with Network Watcher help users understand, diagnose, and gain insights to the network in Azure.	
25	**Ensure that Public IP addresses are Evaluated on a Periodic Basis (Manual)** Public IP Addresses provide tenant accounts with Internet connectivity for resources contained within the tenant. During the creation of certain resources in Azure, a Public IP Address may be created. All Public IP Addresses within the tenant should be periodically reviewed for accuracy and necessity.	Public IP Addresses allocated to the tenant should be periodically reviewed for necessity. Public IP Addresses that are not intentionally assigned and controlled present a publicly facing vector for threat actors and significant risk to the tenant.	
26	**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.	

Sr. No	Control	Risk	Auditors Remarks
27	**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.	
28	**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	
29	**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.	
30	**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.	
31	**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.	
32	**[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."	

Sr. No	Control	Risk	Auditors Remarks
33	**Ensure that the Expiration Date is set for all Keys in RBAC Key Vaults (Automated)** Ensure that all Keys in Role Based Access Control (RBAC) Azure Key Vaults have an expiration date set.	Azure Key Vault enables users to store and use cryptographic keys within the Microsoft Azure environment. The exp (expiration date) attribute identifies the expiration date on or after which the key MUST NOT be used for encryption of new data, wrapping of new keys, and signing. By default, keys never expire. It is thus recommended that keys be rotated in the key vault and set an explicit expiration date for all keys to help enforce the key rotation. This ensures that the keys cannot be used beyond their assigned lifetimes.	
34	**Ensure that the Expiration Date is set for all Keys in Non-RBAC Key Vaults. (Automated)** Ensure that all Keys in Non Role Based Access Control (RBAC) Azure Key Vaults have an expiration date set.	Azure Key Vault enables users to store and use cryptographic keys within the Microsoft Azure environment. The exp (expiration date) attribute identifies the expiration date on or after which the key MUST NOT be used for a cryptographic operation. By default, keys never expire. It is thus recommended that keys be rotated in the key vault and set an explicit expiration date for all keys. This ensures that the keys cannot be used beyond their assigned lifetimes.	
35	**Ensure that the Expiration Date is set for all Secrets in RBAC Key Vaults (Automated)** Ensure that all Secrets in Role Based Access Control (RBAC) Azure Key Vaults have an expiration date set.	The Azure Key Vault enables users to store and keep secrets within the Microsoft Azure environment. Secrets in the Azure Key Vault are octet sequences with a maximum size of 25k bytes each. The exp (expiration date) attribute identifies the expiration date on or after which the secret MUST NOT be used. By default, secrets never expire. It is thus recommended to rotate secrets in the key vault and set an explicit expiration date for all secrets. This ensures that the secrets cannot be used beyond their assigned lifetimes.	
36	**Ensure that the Expiration Date is set for all Secrets in Non-RBAC Key Vaults (Automated)** Ensure that all Secrets in Non Role Based Access Control (RBAC) Azure Key Vaults have an expiration date set.	The Azure Key Vault enables users to store and keep secrets within the Microsoft Azure environment. Secrets in the Azure Key Vault are octet sequences with a maximum size of 25k bytes each. The exp (expiration date) attribute identifies the expiration date on or after which the secret MUST NOT be used. By default, secrets never expire. It is thus recommended to rotate secrets in the key vault and set an explicit expiration date for all secrets. This ensures that the secrets cannot be used beyond their assigned lifetimes.	
37	**Ensure the Key Vault is Recoverable (Automated)** The Key Vault contains object keys, secrets, and certificates. Accidental unavailability of a Key Vault can cause immediate data loss or loss of security functions (authentication, validation, verification, non-repudiation, etc.) supported by the Key Vault objects. It is recommended the Key Vault be made recoverable by enabling the "Do Not Purge" and "Soft Delete" functions. This is in order to prevent loss of encrypted data, including storage accounts, SQL databases, and/or dependent services provided by Key Vault objects (Keys, Secrets, Certificates) etc. This may happen in the case of accidental deletion by a user or from disruptive activity by a malicious user. WARNING: A current limitation of the soft-delete feature across all Azure services is role assignments disappearing when Key Vault is deleted. All role assignments will need to be recreated after	There could be scenarios where users accidentally run delete/purge commands on Key Vault or an attacker/malicious user deliberately does so in order to cause disruption. Deleting or purging a Key Vault leads to immediate data loss, as keys encrypting data and secrets/certificates allowing access/services will become non-accessible. There are 2 Key Vault properties that play a role in permanent unavailability of a Key Vault: 1. enableSoftDelete: Setting this parameter to "true" for a Key Vault ensures that even if Key Vault is deleted, Key Vault itself or its objects remain recoverable for the next 90 days. Key Vault/objects can either be recovered or purged (permanent deletion) during those 90 days. If no action is taken, key vault and its objects will	
38	**Enable Role Based Access Control for Azure Key Vault (Manual)** WARNING: Role assignments disappear when a Key Vault has been deleted (soft-delete) and recovered. Afterwards it will be required to recreate all role assignments. This is a limitation of the soft-delete feature across all Azure services.	The new RBAC permissions model for Key Vaults enables a much finer grained access control for key vault secrets, keys, certificates, etc., than the vault access policy. This in turn will permit the use of privileged identity management over these roles, thus securing the key vaults with JIT Access management.	

Sr. No	Control	Risk	Auditors Remarks
39	**Ensure that Private Endpoints are Used for Azure Key Vault (Manual)** Private endpoints will secure network traffic from Azure Key Vault to the resources requesting secrets and keys.	Private endpoints will keep network requests to Azure Key Vault limited to the endpoints attached to the resources that are whitelisted to communicate with each other. Assigning the Key Vault to a network without an endpoint will allow other resources on that network to view all traffic from the Key Vault to its destination. In spite of the complexity in configuration, this is recommended for high security secrets.	
40	**Ensure Automatic Key Rotation is Enabled Within Azure Key Vault for the Supported Services (Manual)** Automatic Key Rotation is available in Public Preview. The currently supported applications are Key Vault, Managed Disks, and Storage accounts accessing keys within Key Vault. The number of supported applications will incrementally increased.	Once set up, Automatic Private Key Rotation removes the need for manual administration when keys expire at intervals determined by your organization's policy. The recommended key lifetime is 2 years. Your organization should determine its own key expiration policy.	
41	**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.	
42	**Ensure Web App Redirects All HTTP traffic to HTTPS in Azure App Service (Automated)** Azure Web Apps allows sites to run under both HTTP and HTTPS by default. Web 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.	
43	**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.	
44	**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.	
45	**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.	
46	**Ensure That 'PHP version' is the Latest, If Used to Run the Web App (Manual)** Periodically newer versions are released for PHP software either due to security flaws or to include additional functionality. Using the latest PHP version for web apps is recommended in order to take advantage of security fixes, if any, and/or additional functionalities of the newer version.	Newer versions may contain security enhancements and additional functionality. Using the latest software version is recommended in order to take advantage of enhancements and new capabilities. With each software installation, organizations need to determine if a given update meets their requirements. They must also verify the compatibility and support provided for any additional software against the update revision that is selected.	

Sr. No	Control	Risk	Auditors Remarks
47	**Ensure that 'Python version' is the Latest Stable Version, if Used to Run the Web App (Manual)** Periodically, newer versions are released for Python software either due to security flaws or to include additional functionality. Using the latest full Python version for web apps is recommended in order to take advantage of security fixes, if any, and/or additional functionalities of the newer version.	Newer versions may contain security enhancements and additional functionality. Using the latest software version is recommended in order to take advantage of enhancements and new capabilities. With each software installation, organizations need to determine if a given update meets their requirements. They must also verify the compatibility and support provided for any additional software against the update revision that is selected. Using the latest full version will keep your stack secure to vulnerabilities and exploits.	
48	**Ensure that 'Java version' is the latest, if used to run the Web App (Manual)** Periodically, newer versions are released for Java software either due to security flaws or to include additional functionality. Using the latest Java version for web apps is recommended in order to take advantage of security fixes, if any, and/or new functionalities of the newer version.	Newer versions may contain security enhancements and additional functionality. Using the latest software version is recommended in order to take advantage of enhancements and new capabilities. With each software installation, organizations need to determine if a given update meets their requirements. They must also verify the compatibility and support provided for any additional software against the update revision that is selected.	
49	**Ensure that 'HTTP Version' is the Latest, if Used to Run the Web App (Automated)** Periodically, newer versions are released for HTTP either due to security flaws or to include additional functionality. Using the latest HTTP version for web apps to take advantage of security fixes, if any, and/or new functionalities of the newer version.	Newer versions may contain security enhancements and additional functionality. Using the latest version is recommended in order to take advantage of enhancements and new capabilities. With each software installation, organizations need to determine if a given update meets their requirements. They must also verify the compatibility and support provided for any additional software against the update revision that is selected. 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.	
50	**Ensure FTP deployments are Disabled (Automated)** By default, Azure Functions, Web, and API 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 Service Apps and Functions.	Azure FTP deployment endpoints are public. An attacker listening to traffic on a wifi network used by a remote employee or a corporate network could see login traffic in clear-text which would then grant them full control of the code base of the app or service. This finding is more severe if User Credentials for deployment are set at the subscription level rather than using the default Application Credentials which are unique per App.	
51	**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.	

Sr. No	Control	Risk	Auditors Remarks
52	**Ensure that Resource Locks are set for Mission-Critical Azure Resources (Manual)** Resource Manager Locks provide a way for administrators to lock down Azure resources to prevent deletion of, or modifications to, a resource. These locks sit outside of the Role Based Access Controls (RBAC) hierarchy and, when applied, will place restrictions on the resource for all users. These locks are very useful when there is an important resource in a subscription that users should not be able to delete or change. Locks can help prevent accidental and malicious changes or deletion.	As an administrator, it may be necessary to lock a subscription, resource group, or resource to prevent other users in the organization from accidentally deleting or modifying critical resources. The lock level can be set to to CanNotDelete or ReadOnly to achieve this purpose. • CanNotDelete means authorized users can still read and modify a resource, but they cannot delete the resource. • ReadOnly means authorized users can read a resource, but they cannot delete or update the resource. Applying this lock is similar to restricting all authorized users to the permissions granted by the Reader role.	