Azure Cloud Audit Checklist

SACHIN HISSARIA
CA | CISA | DISA | CEH | COBIT-19 | ISO27001:2022 | RPA | Trainer

Sr. No	Control	Risk	Auditors Remarks
1	**Ensure Security Defaults is enabled on Azure Active Directory (Manual)** Security defaults in Azure Active Directory (Azure AD) make it easier to be secure and help protect your organization. Security defaults contain preconfigured security settings for common attacks. Security defaults is available to everyone. The goal is to ensure that all organizations have a basic level of security enabled at no extra cost. You may turn on security defaults in the Azure portal.	Security defaults provide secure default settings that we manage on behalf of organizations to keep customers safe until they are ready to manage their own identity security settings. For example, doing the following: • Requiring all users and admins to register for MFA. • Challenging users with MFA - when necessary, based on factors such as location, device, role, and task. • Disabling authentication from legacy authentication clients, which can't do MFA.	
2	**Ensure that 'Multi-Factor Auth Status' is 'Enabled' for all Privileged Users (Manual)** Enable multi-factor authentication for all roles, groups, and users that have write access or permissions to Azure resources. These include custom created objects or built-in roles such as; • Service Co-Administrators • Subscription Owners • Contributors	Multi-factor authentication requires an individual to present a minimum of two separate forms of authentication before access is granted. Multi-factor authentication provides additional assurance that the individual attempting to gain access is who they claim to be. With multi-factor authentication, an attacker would need to compromise at least two different authentication mechanisms, increasing the difficulty of compromise and thus reducing the risk.	
3	**Ensure that 'Multi-Factor Auth Status' is 'Enabled' for all Non-Privileged Users (Manual)** Enable multi-factor authentication for all non-privileged users.	Multi-factor authentication requires an individual to present a minimum of two separate forms of authentication before access is granted. Multi-factor authentication provides additional assurance that the individual attempting to gain access is who they claim to be. With multi-factor authentication, an attacker would need to compromise at least two different authentication mechanisms, increasing the difficulty of compromise and thus reducing the risk.	
4	**Ensure that 'Allow users to remember multi-factor authentication on devices they trust' is Disabled (Manual)** Do not allow users to remember multi-factor authentication on devices.	Remembering Multi-Factor Authentication (MFA) for devices and browsers allows users to have the option to bypass MFA for a set number of days after performing a successful sign-in using MFA. This can enhance usability by minimizing the number of times a user may need to perform two-step verification on the same device. However, if an account or device is compromised, remembering MFA for trusted devices may affect security. Hence, it is recommended that users not be allowed to bypass MFA.	
5	**Ensure Trusted Locations Are Defined (Manual)** Azure Active Directory Conditional Access allows an organization to configure Named locations and configure whether those locations are trusted or untrusted. These settings provide organizations the means to specify Geographical locations for use in conditional access policies, or define actual IP addresses and IP ranges and whether or not those IP addresses and/or ranges are trusted by the organization.	Defining trusted source IP addresses or ranges helps organizations create and enforce Conditional Access policies around those trusted or untrusted IP addresses and ranges. Users authenticating from trusted IP addresses and/or ranges may have less access restrictions or access requirements when compared to users that try to authenticate to Azure Active Directory from untrusted locations or untrusted source IP addresses/ranges.	
6	**Ensure that an exclusionary Geographic Access Policy is considered (Manual)** CAUTION: If these policies are created without first auditing and testing the result, misconfiguration can potentially lock out administrators or create undesired access issues. Conditional Access Policies can be used to block access from geographic locations that are deemed out-of-scope for your organization or application. The scope and variables for this policy should be carefully examined and defined.	Conditional Access, when used as a deny list for the tenant or subscription, is able to prevent ingress or egress of traffic to countries that are outside of the scope of interest (e.g.: customers, suppliers) or jurisdiction of an organization. This is an effective way to prevent unnecessary and long-lasting exposure to international threats such as APTs.	
7	**Ensure that A Multi-factor Authentication Policy Exists for Administrative Groups (Manual)** For designated users, they will be prompted to use their multi-factor authentication (MFA) process on login.	Enabling multi-factor authentication is a recommended setting to limit the use of Administrative accounts to authenticated personnel.	
8	**Ensure that A Multi-factor Authentication Policy Exists for All Users (Manual)** For designated users, they will be prompted to use their multi-factor authentication (MFA) process on logins.	Enabling multi-factor authentication is a recommended setting to limit the potential of accounts being compromised and limiting access to authenticated personnel.	

Sr. No	Control	Risk	Auditors Remarks
9	**Ensure Multi-factor Authentication is Required for Risky Sign-ins (Manual)** For designated users, they will be prompted to use their multi-factor authentication (MFA) process on login.	Enabling multi-factor authentication is a recommended setting to limit the potential of accounts being compromised and limiting access to authenticated personnel.	
10	**Ensure Multi-factor Authentication is Required for Azure Management (Manual)** For designated users, they will be prompted to use their multi-factor authentication (MFA) process on logins.	Enabling multi-factor authentication is a recommended setting to limit the use of Administrative actions and to prevent intruders from changing settings.	
11	**Ensure that 'Users can create Azure AD Tenants' is set to 'No' (Automated)** Require administrators or appropriately delegated users to create new tenants.	It is recommended to only allow an administrator to create new tenants. This prevent users from creating new Azure AD or Azure AD B2C tenants and ensures that only authorized users are able to do so.	
12	**Ensure Access Review is Set Up for External Users in Azure AD Privileged Identity Management (Manual)** This recommendation extends guest access review by utilizing the Azure AD Privileged Identity Management feature provided in Azure AD Premium P2. Azure AD is extended to include Azure AD B2B collaboration, allowing you to invite people from outside your organization to be guest users in your cloud account and sign in with their own work, school, or social identities. Guest users allow you to share your company's applications and services with users from any other organization, while maintaining control over your own corporate data. Work with external partners, large or small, even if they don't have Azure AD or an IT department. A simple invitation and redemption process lets partners use their own credentials to access your company's resources a a guest user.	Guest users in the Azure AD are generally required for collaboration purposes in Office 365, and may also be required for Azure functions in enterprises with multiple Azure tenants. Guest users should be reviewed on a regular basis, at least annually. Guest users should not be granted administrative roles where possible. Guest users are typically added outside your employee on-boarding/off-boarding process and could potentially be overlooked indefinitely, leading to a potential vulnerability. Guest users should be reviewed on a monthly basis to ensure that inactive and unneeded accounts are removed.	
13	**Ensure Guest Users Are Reviewed on a Regular Basis (Manual)** Azure AD is extended to include Azure AD B2B collaboration, allowing you to invite people from outside your organization to be guest users in your cloud account and sign in with their own work, school, or social identities. Guest users allow you to share your company's applications and services with users from any other organization, while maintaining control over your own corporate data. Work with external partners, large or small, even if they don't have Azure AD or an IT department. A simple invitation and redemption process lets partners use their own credentials to access your company's resources as a guest user. Guest users in every subscription should be review on a regular basis to ensure that inactive and unneeded accounts are removed.	Guest users in the Azure AD are generally required for collaboration purposes in Office 365, and may also be required for Azure functions in enterprises with multiple Azure tenants. Guest users are typically added outside your employee on-boarding/off-boarding process and could potentially be overlooked indefinitely, leading to a potential vulnerability. To prevent this, guest users should be reviewed on a regular basis. During this audit, guest users should also be determined to not have administrative privileges.	
14	**Ensures that two alternate forms of identification are provided before allowing a password reset.** A Self-service Password Reset (SSPR) through Azure Multi-factor Authentication (MFA) ensures the user's identity is confirmed using two separate methods of identification. With multiple methods set, an attacker would have to compromise both methods before they could maliciously reset a user's password.	There may be administrative overhead, as users who lose access to their secondary authentication methods will need an administrator with permissions to remove it. There will also need to be organization-wide security policies and training to teach administrators to verify the identity of the requesting user so that social engineering can not render this setting useless.	
15	**Ensure that a Custom Bad Password List is set to 'Enforce' for your Organization (Manual)** Microsoft Azure provides a Global Banned Password policy that applies to Azure administrative and normal user accounts. This is not applied to user accounts that are synced from an on-premise Active Directory unless Azure AD Connect is used and you enable EnforceCloudPasswordPolicyForPasswordSyncedUsers. Please see the list in default values on the specifics of this policy. To further password security, it is recommended to further define a custom banned password policy.	Enabling this gives your organization further customization on what secure passwords are allowed. Setting a bad password list enables your organization to fine-tune its password policy further, depending on your needs. Removing easy-to-guess passwords increases the security of access to your Azure resources.	

Sr. No	Control	Risk	Auditors Remarks
16	**Ensure that 'Number of days before users are asked to re-confirm their authentication information' is not set to '0' (Manual)** Ensure that the number of days before users are asked to re-confirm their authentication information is not set to 0.	This setting is necessary if you have setup 'Require users to register when signing in option'. If authentication re-confirmation is disabled, registered users will never be prompted to re-confirm their existing authentication information. If the authentication information for a user changes, such as a phone number or email, then the password reset information for that user reverts to the previously registered authentication information.	
17	**Ensure that 'Notify users on password resets?' is set to 'Yes' (Manual)** Ensure that users are notified on their primary and secondary emails on password resets.	User notification on password reset is a proactive way of confirming password reset activity. It helps the user to recognize unauthorized password reset activities.	
18	**Ensure That 'Notify all admins when other admins reset their password?' is set to 'Yes' (Manual)** Ensure that all Global Administrators are notified if any other administrator resets their password.	Global Administrator accounts are sensitive. Any password reset activity notification, when sent to all Global Administrators, ensures that all Global administrators can passively confirm if such a reset is a common pattern within their group. For example, if all Global Administrators change their password every 30 days, any password reset activity before that may require administrator(s) to evaluate any unusual activity and confirm its origin.	
19	**Ensure `User consent for applications` is set to `Do not allow user consent` (Manual)** Require administrators to provide consent for applications before use.	If Azure Active Directory is running as an identity provider for third-party applications, permissions and consent should be limited to administrators or pre-approved. Malicious applications may attempt to exfiltrate data or abuse privileged user accounts.	
20	**Ensure ‘User consent for applications’ Is Set To ‘Allow for Verified Publishers’ (Manual)** Allow users to provide consent for selected permissions when a request is coming from a verified publisher.	If Azure Active Directory is running as an identity provider for third-party applications, permissions and consent should be limited to administrators or pre-approved. Malicious applications may attempt to exfiltrate data or abuse privileged user accounts.	
21	**Ensure that 'Users can add gallery apps to My Apps' is set to 'No' (Manual)** Require administrators to provide consent for the apps before use.	Unless Azure Active Directory is running as an identity provider for third-party applications, do not allow users to use their identity outside of your cloud environment. User profiles contain private information such as phone numbers and email addresses which could then be sold off to other third parties without requiring any further consent from the user.	
22	**Ensure That ‘Users Can Register Applications’ Is Set to ‘No’ (Manual)** Require administrators or appropriately delegated users to register third-party applications.	It is recommended to only allow an administrator to register custom-developed applications. This ensures that the application undergoes a formal security review and approval process prior to exposing Azure Active Directory data. Certain users like developers or other high-request users may also be delegated permissions to prevent them from waiting on an administrative user. Your organization should review your policies and decide your needs.	
23	**Ensure That 'Guest users access restrictions' is set to 'Guest user access is restricted to properties and memberships of their own directory objects' (Manual)** Limiting guest access ensures that guest accounts do not have permission for certain directory tasks, such as enumerating users, groups or other directory resources, and cannot be assigned to administrative roles in your directory. Guest access has three levels of restriction. 1. Guest users have the same access as members (most inclusive), 2. Guest users have limited access to properties and memberships of directory objects (default value), 3. Guest user access is restricted to properties and memberships of their own directory objects (most restrictive). The recommended option is the 3rd, most restrictive: "Guest user access is restricted to their own directory object".	This may create additional requests for permissions to access resources that administrators will need to approve.	

Sr. No	Control	Risk	Auditors Remarks
24	**Ensure that 'Guest invite restrictions' is set to "Only users assigned to specific admin roles can invite guest users" (Manual)** Restrict invitations to users with specific administrative roles only.	Restricting invitations to users with specific administrator roles ensures that only authorized accounts have access to cloud resources. This helps to maintain "Need to Know" permissions and prevents inadvertent access to data. By default the setting Guest invite restrictions is set to Anyone in the organization can invite guest users including guests and non-admins. This would allow anyone within the organization to invite guests and non-admins to the tenant, posing a security risk.	
25	**Ensure That 'Restrict access to Azure AD administration portal' is Set to 'Yes' (Manual)** Restrict access to the Azure AD administration portal to administrators only. **NOTE:** This only affects access to the Azure AD administrator's web portal. This setting does not prohibit privileged users from using other methods such as Rest API or Powershell to obtain sensitive information from Azure AD.	The Azure AD administrative portal has sensitive data and permission settings. All non-administrators should be prohibited from accessing any Azure AD data in the administration portal to avoid exposure.	
26	**Ensure that 'Restrict user ability to access groups features in the Access Pane' is Set to 'Yes' (Manual)** Restricts group creation to administrators with permissions only.	Self-service group management enables users to create and manage security groups or Office 365 groups in Azure Active Directory (Azure AD). Unless a business requires this day-to-day delegation for some users, self-service group management should be disabled.	
27	**Ensure that 'Users can create security groups in Azure portals, API or PowerShell' is set to 'No' (Manual)** Restrict security group creation to administrators only.	When creating security groups is enabled, all users in the directory are allowed to create new security groups and add members to those groups. Unless a business requires this day-to-day delegation, security group creation should be restricted to administrators only.	
28	**Ensure that 'Owners can manage group membership requests in the Access Panel' is set to 'No' (Manual)** Restrict security group management to administrators only.	Restricting security group management to administrators only prohibits users from making changes to security groups. This ensures that security groups are appropriately managed and their management is not delegated to non-administrators.	
29	**Ensure that 'Users can create Microsoft 365 groups in Azure portals, API or PowerShell' is set to 'No' (Manual)** Restrict Microsoft 365 group creation to administrators only.	Restricting Microsoft 365 group creation to administrators only ensures that creation of Microsoft 365 groups is controlled by the administrator. Appropriate groups should be created and managed by the administrator and group creation rights should not be delegated to any other user.	
30	**Ensure that 'Require Multi-Factor Authentication to register or join devices with Azure AD' is set to 'Yes' (Manual)** Joining or registering devices to the active directory should require Multi-factor authentication.	Multi-factor authentication is recommended when adding devices to Azure AD. When set to Yes, users who are adding devices from the internet must first use the second method of authentication before their device is successfully added to the directory. This ensures that rogue devices are not added to the domain using a compromised user account. Note: Some Microsoft documentation suggests to use conditional access policies for joining a domain from certain whitelisted networks or devices. Even with these in place, using Multi-Factor Authentication is still recommended, as it creates a process for review before joining the domain.	
31	**Ensure That No Custom Subscription Administrator Roles Exist (Automated)** The principle of least privilege should be followed and only necessary privileges should be assigned instead of allowing full administrative access.	Classic subscription admin roles offer basic access management and include Account Administrator, Service Administrator, and Co-Administrators. It is recommended the least necessary permissions be given initially. Permissions can be added as needed by the account holder. This ensures the account holder cannot perform actions which were not intended.	

Sr. No	Control	Risk	Auditors Remarks
32	**Ensure a Custom Role is Assigned Permissions for Administering Resource Locks (Manual)** Resource locking is a powerful protection mechanism that can prevent inadvertent modification/deletion of resources within Azure subscriptions/Resource Groups and is a recommended NIST configuration.	Given the resource lock functionality is outside of standard Role Based Access Control(RBAC), it would be prudent to create a resource lock administrator role to prevent inadvertent unlocking of resources.	
33	**Ensure That 'Subscription Entering AAD Directory' and 'Subscription Leaving AAD Directory' Is Set To 'Permit No One' (Manual)** Users who are set as subscription owners are able to make administrative changes to the subscriptions and move them into and out of Azure Active Directories.	Permissions to move subscriptions in and out of Azure Active Directory must only be given to appropriate administrative personnel. A subscription that is moved into an Azure Active Directory may be within a folder to which other users have elevated permissions. This prevents loss of data or unapproved changes of the objects within by potential bad actors.	
34	**Ensure That Microsoft Defender for Servers Is Set to 'On' (Manual)** Turning on Microsoft Defender for Servers enables threat detection for Servers, providing threat intelligence, anomaly detection, and behavior analytics in the Microsoft Defender for Cloud.	Enabling Microsoft Defender for Servers allows for greater defense-in-depth, with threat detection provided by the Microsoft Security Response Center (MSRC).	
35	**Ensure That Microsoft Defender for App Services Is Set To 'On' (Manual)** Turning on Microsoft Defender for App Service enables threat detection for App Service, providing threat intelligence, anomaly detection, and behavior analytics in the Microsoft Defender for Cloud.	Enabling Microsoft Defender for App Service allows for greater defense-in-depth, with threat detection provided by the Microsoft Security Response Center (MSRC).	
36	**Ensure That Microsoft Defender for Databases Is Set To 'On' (Manual)** Turning on Microsoft Defender for Databases enables threat detection for the instances running your database software. This provides threat intelligence, anomaly detection, and behavior analytics in the Azure Microsoft Defender for Cloud. Instead of being enabled on services like Platform as a Service (PaaS), this implementation will run within your instances as Infrastructure as a Service (IaaS) on the Operating Systems hosting your databases.	Enabling Microsoft Defender for Azure SQL Databases allows your organization more granular control of the infrastructure running your database software. Instead of waiting on Microsoft release updates or other similar processes, you can manage them yourself. Threat detection is provided by the Microsoft Security Response Center (MSRC).	
37	**Ensure That Microsoft Defender for Azure SQL Databases Is Set To 'On' (Manual)** Turning on Microsoft Defender for Azure SQL Databases enables threat detection for Azure SQL database servers, providing threat intelligence, anomaly detection, and behavior analytics in the Microsoft Defender for Cloud.	Enabling Microsoft Defender for Azure SQL Databases allows for greater defense-in-depth, with threat detection provided by the Microsoft Security Response Center (MSRC).	
38	**Ensure That Microsoft Defender for SQL Servers on Machines Is Set To 'On' (Manual)** Turning on Microsoft Defender for SQL servers on machines enables threat detection for SQL servers on machines, providing threat intelligence, anomaly detection, and behavior analytics in the Microsoft Defender for Cloud.	Enabling Microsoft Defender for SQL servers on machines allows for greater defense-in-depth, with threat detection provided by the Microsoft Security Response Center (MSRC).	
39	**Ensure That Microsoft Defender for Open-Source Relational Databases Is Set To 'On' (Manual)** Turning on Microsoft Defender for Open-source relational databases enables threat detection for Open-source relational databases, providing threat intelligence, anomaly detection, and behavior analytics in the Microsoft Defender for Cloud.	Enabling Microsoft Defender for Open-source relational databases allows for greater defense-in-depth, with threat detection provided by the Microsoft Security Response Center (MSRC).	
40	**Ensure That Microsoft Defender for Storage Is Set To 'On' (Manual)** Turning on Microsoft Defender for Storage enables threat detection for Storage, providing threat intelligence, anomaly detection, and behavior analytics in the Microsoft Defender for Cloud.	Enabling Microsoft Defender for Storage allows for greater defense-in-depth, with threat detection provided by the Microsoft Security Response Center (MSRC).	
41	**Ensure That Microsoft Defender for Containers Is Set To 'On' (Manual)** Turning on Microsoft Defender for Containers enables threat detection for Container Registries including Kubernetes, providing threat intelligence, anomaly detection, and behavior analytics in the Microsoft Defender for Cloud.	Enabling Microsoft Defender for Container Registries allows for greater defense-in-depth, with threat detection provided by the Microsoft Security Response Center (MSRC).	

Sr. No	Control	Risk	Auditors Remarks
42	**Ensure That Microsoft Defender for Azure Cosmos DB Is Set To 'On' (Manual)** Microsoft Defender for Azure Cosmos DB scans all incoming network requests for threats to your Azure Cosmos DB resources.	In scanning Azure Cosmos DB requests within a subscription, requests are compared to a heuristic list of potential security threats. These threats could be a result of a security breach within your services, thus scanning for them could prevent a potential security threat from being introduced.	
43	**Ensure That Microsoft Defender for Key Vault Is Set To 'On' (Manual)** Turning on Microsoft Defender for Key Vault enables threat detection for Key Vault, providing threat intelligence, anomaly detection, and behavior analytics in the Microsoft Defender for Cloud.	Enabling Microsoft Defender for Key Vault allows for greater defense-in-depth, with threat detection provided by the Microsoft Security Response Center (MSRC).	
44	**Ensure That Microsoft Defender for DNS Is Set To 'On' (Manual)** Microsoft Defender for DNS scans all network traffic exiting from within a subscription.	DNS lookups within a subscription are scanned and compared to a dynamic list of websites that might be potential security threats. These threats could be a result of a security breach within your services, thus scanning for them could prevent a potential security threat from being introduced.	
45	**Ensure That Microsoft Defender for Resource Manager Is Set To 'On' (Manual)** Microsoft Defender for Resource Manager scans incoming administrative requests to change your infrastructure from both CLI and the Azure portal.	Scanning resource requests lets you be alerted every time there is suspicious activity in order to prevent a security threat from being introduced.	
46	**Ensure that Microsoft Defender Recommendation for 'Apply system updates' status is 'Completed' (Manual)** Ensure that the latest OS patches for all virtual machines are applied.	Windows and Linux virtual machines should be kept updated to: • Address a specific bug or flaw • Improve an OS or application’s general stability • Fix a security vulnerability The Azure Security Center retrieves a list of available security and critical updates from Windows Update or Windows Server Update Services (WSUS), depending on which service is configured on a Windows VM. The security center also checks for the latest updates in Linux systems. If a VM is missing a system update, the security center will recommend system updates be applied.	
47	**Ensure Any of the ASC Default Policy Settings are Not Set to 'Disabled' (Manual)** None of the settings offered by ASC Default policy should be set to effect Disabled.	A security policy defines the desired configuration of your workloads and helps ensure compliance with company or regulatory security requirements. ASC Default policy is associated with every subscription by default. ASC default policy assignment is a set of security recommendations based on best practices. Enabling recommendations in ASC default policy ensures that Azure security center provides the ability to monitor all of the supported recommendations and optionally allow automated action for a few of the supported recommendations.	
48	**Ensure that Auto provisioning of 'Log Analytics agent for Azure VMs' is Set to 'On' (Automated)** Enable automatic provisioning of the monitoring agent to collect security data.	When Log Analytics agent for Azure VMs is turned on, Microsoft Defender for Cloud provisions the Microsoft Monitoring Agent on all existing supported Azure virtual machines and any new ones that are created. The Microsoft Monitoring Agent scans for various security-related configurations and events such as system updates, OS vulnerabilities, endpoint protection, and provides alerts.	
49	**Ensure that Auto provisioning of 'Vulnerability assessment for machines' is Set to 'On' (Manual)** Enable automatic provisioning of vulnerability assessment for machines on both Azure and hybrid (Arc enabled) machines.	Vulnerability assessment for machines scans for various security-related configurations and events such as system updates, OS vulnerabilities, and endpoint protection, then produces alerts on threat and vulnerability findings.	
50	**Ensure that Auto provisioning of 'Microsoft Defender for Containers components' is Set to 'On' (Manual)** Enable automatic provisioning of the Microsoft Defender for Containers components.	As with any compute resource, Container environments require hardening and run-time protection to ensure safe operations and detection of threats and vulnerabilities.	

Sr. No	Control	Risk	Auditors Remarks

IF YOU FIND THIS USEFUL , SHARE WITH YOUR NETWORK.

FOLLOW FOR MORE SUCH CHECKLIST | TEMPLATE | IT AUDIT RELATED STUFF

https://www.linkedin.com/in/sachin-hissaria/

https://youtube.com/@sachinhissaria6512