Audit Checklist

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

Sr. No	Control	Risk	Status	Auditors Remarks
1	**Ensure Administration of WorkSpaces is defined using IAM (Manual)** To allow users to administer Amazon WorkSpaces, IAM policies must be created and attached with the required permissions to an IAM Principal used for administration of Amazon WorkSpaces. An IAM Principal may be a IAM Role or an IAM User, or an IAM User Group with Users within the User Group. AWS has an AWS Managed Policy, AmazonWorkSpacesAdmin that grants permissions to administer Amazon WorkSpaces. A custom managed policy or inline policy may be used to grant WorkSpaces permissions to the IAM Principal	Creating and managing Workspaces specific users is not done in AWS IAM. Creating and managing Workspaces specific users is done within the Workspace service console. In order to properly administer Workspaces specific users, an IAM Principal with proper permissions must be created.		
2	**Ensure MFA is enabled for WorkSpaces users (Manual)** Multi-Factor Authentication (MFA) adds an extra layer of authentication assurance beyond traditional username and password. With MFA enabled, when a user signs in to Amazon WorkSpaces, they will be prompted for their user name and password as well as for an authentication code from their physical or virtual MFA token. It is recommended that MFA be enabled for all accounts that utilize WorkSpaces.	Enabling MFA provides increased security to a username and password as it requires the user to have a virtual or physical hardware solution that displays a time-sensitive code.		
3	**Ensure WorkSpace volumes are encrypted. (Automated)** Encrypt WorkSpaces root volume (C:drive for Windows and root for Amazon Linux) and user volume (D:drive for Windows and /home for Amazon Linux).	When you launch a WorkSpace, you can encrypt the root volume and the user volume. This ensures that the data stored at rest for WorkSpaces is encrypted.		
4	**Ensure WorkSpaces are deployed in their own virtual private cloud (VPC) (Manual)** Amazon WorkSpaces VPC should be created with two private subnets for your WorkSpaces and a NAT gateway in a public subnet.	The NAT gateway will provide WorkSpaces access to the internet for updates to the operating system and so that applications can be deployed using Amazon WorkSpaces Application Manager if that is applicable for your environment.		
5	**Ensure WorkSpaces traffic is controlled and routed through a NAT Gateway. (Manual)** A network address translation (NAT) gateway enables instances in a private subnet to connect to the internet or other AWS services, but prevents the internet from initiating a direct connection with those instances.	WorkSpaces must have access to the internet so that you can install updates to the operating system and deploy applications.		
6	**Ensure Web Access to Workspaces is Disabled (Automated)** WorkSpaces access should be restricted to trusted operating systems and clients	WorkSpaces access is supported from a variety of clients and operating systems, including HTML5 based browsers. Disabling Web Access prevents access to the Workspace from HTML5 based browsers, ensuring access can only occur from known operating systems.		
7	**Ensure access is limited to trusted devices (Manual)** WorkSpaces access should be restricted to trusted devices with valid certificates.	WorkSpaces is accessible from any supported device that is connected to the internet. When you enable access to trusted devices, Amazon WorkSpaces uses certificate-based authentication to determine whether a device is trusted.		
8	**Ensure the default IP access control group is disassociated. (Automated)** The default IP Access Control group allows all traffic. Once you create and attach an IP Access Control Group the default is disassociated.	IP Access Control group acts as a virtual firewall for your WorkSpaces allowing you to add your trusted networks.		

Sr. No	Control	Risk	Status	Auditors Remarks
9	**Ensure CloudWatch is set up for WorkSpaces (Manual)** Set up and utilize Amazon CloudWatch Events for successful logins to WorkSpaces.	Use Cloudwatch to store/archive WorkSpaces login events for future reference, analysis, and action based on the patterns. Utilize the IP address collected to figure out where users are logged in from, and then build policies to allow access only to files or data from those WorkSpaces that meet company access criteria. With this information you can also use policy controls to block access from unauthorized IP addresses.		
10	**Ensure that patches and updates are performed on the operating system for Workstations (Automated)** In order for Windows updates to occur auto-stop WorkSpaces must be utilized and the default for maintenance mode must be set to enabled.	Windows Operating systems updates can be a high security vulnerability and normal updates and patches can help eliminate these vulnerabilities.		
11	**Ensure your WorkSpaces image has the appropriate CIS Operating System Benchmark applied (Manual)** Utilize the CIS Benchmark to secure the Operating system image that you are utilizing for your WorkSpaces.	Securing the Operating system with a CIS Benchmark ensures all systems remain in a secure, compliant and hardened state.		
12	**Restrict WorkSpaces Bundle options to organization approved versions (Manual)** Limit the existing WorkSpaces bundles that can be utilized and provisioned within your AWS account.	Limiting the type of AWS WorkSpaces bundle that can be utilized can address internal security and compliance requirements.		
13	**Ensure Workspaces images are not older than 90 days. (Manual)** WorkSpaces images should not have a creation time stamp over 90 days.	WorkSpaces images require Operating system patches to be applied and updated and by confirming the creation date is not over 90 days old can help ensure that updates are being applied.		
14	**Ensure WorkSpaces that are not being utilized are removed. (Automated)** Identify and remove any WorkSpace instances available within your AWS account that are not being utilized.	An AWS WorkSpaces instance is considered unused if has 0 (zero) known user connections registered within the past 30 days.		
15	**Ensure primary interface ports for Workspaces are not open to all inbound traffic. (Automated)** Ensure that the inbound traffic of the primary network interface for all WorkSpaces is not open to all connections 0.0.0.0\00.	Attached security groups to the primary elastic network interface (ENI) to manage ports and network communication should not be open to all communication. They should be restricted to what is required by WorkSpaces, the Organization and other services.		
16	**Ensure FIPS Endpoint encryption is enabled for WorkSpaces. (Manual)** To meet a high level of security and comply with different compliance standards, you must use Federal Information Processing Standards (FIPS) endpoint encryption at the directory level with WorkSpaces.	You must also use an AWS Region that is authorized for the same compliance standard that you are trying to achieve.		
17	**Ensure WorkSpaces API requests flow through a VPC Endpoint (Automated)** For any WorkSpaces API requests setup the connection through an interface endpoint in your VPC.	Utilizing a VPC interface endpoint for WorkSpaces API requests keeps the communication within the AWS network.		
18	**Ensure Radius server is using the recommended security protocol (Automated)** The authentication protocol between the Microsoft AD DCs and the RADIUS server supported are PAP, CHAP, MS-CHAPv1, and MS-CHAPv2.	MS-CHAPv2 provides the strongest security of the options supported.		

Sr. No	Control	Risk	Status	Auditors Remarks
19	**Ensure User Access Logging is enabled (Manual)** User Access Logging can record the following user events: • Session Start - when a WorkSpaces Web sessions begins. • Session End - when a WorkSpaces Web session ends. • URL Navigation - when a user loads a URL. User Access logging can be setup to record user events.	Logging user activity will assist in event correlation if response to an incident is needed.		
20	**Ensure Administrators of WorkDocs is defined using IAM (Automated)** To allow users to administer Amazon WorkDocs resources, you must create an IAM policy that explicitly grants them the correct permissions. This policy should then be attached to the group or role defined for this administration.	WorkDocs Administrators control access and authorization for users of the WorkDocs resources.		
21	**Ensure MFA is enabled for WorkDoc users (Manual)** Multi-Factor Authentication (MFA) adds an extra layer of authentication assurance beyond traditional username and password. With MFA enabled, when a user signs in to Amazon WorkDocs, they will be prompted for their user name and password as well as for an authentication code from their MFA token.	Enabling MFA provides increased security to a user name and password as it requires the user to possess a solution that displays a time-sensitive authentication code.		
22	**Ensure Workdocs access is limited to a range of allowable IP addresses (Manual)** Access to WorkDocs can be limited to an allowed range of IP addresses.	Using IP address allow lists, you define and permit access to your WorkDocs site from trusted networks.		
23	**Utilize site wide activity feed for monitoring. (Manual)** Admins can view and export the activity feed for an entire WorkDocs site.	WorkDoc admins should monitor and export activity feeds for the site as record of activity. These activity reports should be reviewed every month for any abnormalities and rotated every 90 days.		
24	**Ensure new users can only be invited from allowed domains. (Manual)** Users that are allowed access to shared files or folders in WorkDocs should be limited to specific domains.	To control who should be allowed to join your WorkDocs site, users should be limited on who they can invite sharing files or folders with new people from the specified domains.		
25	**Ensure only specific users are allowed to invite external users (Manual)** The organization should only allow administrators the ability to invite external users to the WorkDocs site.	If anyone can invite a user outside of the organization it could potentially lead to security or information leak.		
26	**Ensure publicly shareable links is not allowed in WorkDocs (Manual)** The organization should not allow publicly shareable links for WorkDocs.	If a user can create and send a publicly shareable links allowing a file to be viewed by people outside of the organization it could potentially lead to an security or information leak.		
27	**Ensure any user that has not accessed WorkDocs in 30 days is set to inactive. (Manual)** User accounts that are not actively using the WorkDocs service should be set to inactive after a period of 30 days.	Inactive accounts may appear to not pose a problem but they can provide unauthorized access to files within WorkDocs.		
28	**Ensure AppStream is utilizing its own virtual private cloud (VPC) (Manual)** AppStream 2.0 should be configured using a VPC with Private subnets and a NAT Gateway.	For AppStream 2.0 the public subnet will have direct access to the internet through the NAT gateway. This setup allows the streaming instances in your private subnets to connect to the internet or other AWS services.		

Sr. No	Control	Risk	Status	Auditors Remarks
29	**Ensure a VPC Endpoint is set for AppStream (Manual)** When you select Using a VPC endpoint, this allows users to only stream from this AppStream 2.0 stack when they have network access to the VPC.	Virtual Private Cloud (VPC) endpoints allow your users to stream from AppStream 2.0 through your VPC. You can create a VPC endpoint in the VPC of your choosing, then use the endpoint with AppStream 2.0 VPC to maintain the streaming traffic within the VPC.		
30	**Ensure maximum session duration is no longer than 10 hours (Automated)** When creating a fleet for AppStream 2.0 configure the Maximum session duration in minutes to be no greater than 600.	Having a session duration lasting longer than 10 hours should not be necessary and if running for any malicious reasons provides a greater time for usage than should be allowed.		
31	**Ensure session disconnect timeout is set to 5 minutes or less (Automated)** Disconnect timeout in minutes, is the amount of of time that a streaming session remains active after users disconnect.	If users try to reconnect to the streaming session after a disconnection or network interruption within the 5 minutes, they are connected to their previous session. Otherwise, they are connected to a new session with a new streaming instance and that instance isn't sitting out there not being used.		
32	**Ensure session Idle disconnect timeout is set to 10 minutes or less (Automated)** Idle disconnect timeout in minutes is the amount of time that users can be inactive before they are disconnected from their streaming session and the Disconnect timeout in minutes time begins.	Users are considered idle when they stop providing keyboard or mouse input during their streaming session. File uploads and downloads, audio in, audio out, and pixels changing do not qualify as user activity. Once disconnected from their streaming session the Disconnect timeout begins.		
33	**Ensure internet access is granted and managed through your VPC (Automated)** Default Internet Access from your fleet streaming instances should remain unchecked.	When Default Internet Access is enabled, AppStream 2.0 uses the internet gateway in the VPC public subnet to connect to the public internet. The streaming instances are then assigned public IP addresses that are directly accessible from the internet. Internet Access from fleet streaming instances should be controlled using a NAT gateway in the VPC. When Default Internet Access is not enabled, streaming instances are assigned a private IP address that are not directly accessible from the internet.		
34	**Ensure Operating system updates are applied to your base image every 30 days. (Manual)** To ensure that your fleet instances have the latest Windows updates installed, we recommend that you install Windows updates on your image builder, create a new image, and then update your fleet with the new image once a month.	All fleet instances used in user streaming sessions have only the Windows and application updates that were installed on the underlying image when it was created. In addition, any updates made to Windows or to applications on the instance during the streaming session will not persist to future sessions by the same user or other users.		