Audit Checklist

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

Sr. No	Control	Risk	Status	Auditors Remarks
1	**Ensure Consistent Naming Convention is used for Organizational AMI (Manual)** The naming convention for AMI (Amazon Machine Images) should be documented and followed for any AMI's created	The majority of AWS resources can be named and tagged. Most organizations have already created standardize naming conventions, and have existing rules in effect. They simply need to extend that for all AWS cloud resources to include Amazon Machine Images (AMI)		
2	**Ensure Images (AMI's) are encrypted (Manual)** Amazon Machine Images should utilize EBS Encrypted snapshots	AMIs backed by EBS snapshots should use EBS encryption. Snapshot volumes can be encrypted and attached to an AMI.		
3	**Ensure Only Approved AMIs (Images) are Used (Manual)** Ensure that all base AMIs utilized are approved for use by your organization.	An approved AMI is a base EC2 machine image that is a pre-configured OS configured to run your application. Using approved AMIs helps enforce consistency and security.		
4	**Ensure Images (AMI) are not older than 90 days (Manual)** Ensure that your AMIs are not older than 90 days.	Using up-to-date AMIs will provide many benefits from OS updates and security patches helping to ensure reliability, security and compliance.		
5	**Ensure Images are not Publicly Available (Manual)** EC2 allows you to make an AMI public, sharing it with all AWS accounts.	Publicly sharing an AMI with all AWS accounts could expose organizational data and configuration information.		
6	**Ensure EBS volume encryption is enabled (Automated)** Elastic Compute Cloud (EC2) supports encryption at rest when using the Elastic Block Store (EBS) service. While disabled by default, forcing encryption at EBS volume creation is supported.	Encrypting data at rest reduces the likelihood that it is unintentionally exposed and can nullify the impact of disclosure if the encryption remains unbroken.		
7	**Ensure Public Access to EBS Snapshots is Disabled** To protect your data disable the public mode of EBS snapshots.	This protects your data so that it is not accessible to all AWS accounts preventing accidental access and leaks.		
8	**Ensure EBS volume snapshots are encrypted (Manual)** Elastic Compute Cloud (EC2) supports encryption at rest when using the Elastic Block Store (EBS) service.	Encrypting data at rest reduces the likelihood that it is unintentionally exposed and can nullify the impact of disclosure if the encryption remains unbroken.		
9	**Ensure unused EBS volumes are removed (Manual)** Identify any unused Elastic Block Store (EBS) volumes in your AWS account and remove them.	Any Elastic Block Store volume created in your AWS account contains data, regardless of being used or not. If you have EBS volumes (other than root volumes) that are unattached to an EC2 instance they should be removed to prevent unauthorized access or data leak to any sensitive data on these volumes.		
10	**Ensure Tag Policies are Enabled (Manual)** Tag policies help you standardize tags on all tagged resources across your organization.	You can use tag policies to define tag keys (including how they should be capitalized) and their allowed values.		
11	**Ensure an Organizational EC2 Tag Policy has been Created (Manual)** A tag policy enables you to define tag compliance rules to help you maintain consistency in the tags attached to your organization's resources.	You can use an EC2 tag policy to enforce your tag strategy across all of your EC2 resources.		
12	**Ensure no AWS EC2 Instances are Older than 180 days (Manual)** Identify any running AWS EC2 instances older than 180 days.	An EC2 instance is not supposed to run indefinitely and having instance older than 180 days can increase the risk of problems and issues.		
13	**Ensure detailed monitoring is enable for production EC2 Instances (Manual)** Ensure that detailed monitoring is enabled for your Amazon EC2 instances.	Monitoring is an important part of maintaining the reliability, availability, and performance of your Amazon EC2 instances		

Sr. No	Control	Risk	Status	Auditors Remarks
14	**Ensure Default EC2 Security groups are not being used. (Manual)** When an EC2 instance is launched a specified custom security group should be assigned to the instance.	When an EC2 Instance is launched the default security group is automatically assigned. In error a lot of instances are launched in this way, and if the default security group is configured to allow unrestricted access, it will increase the attack footprint allowing the opportunity for malicious activity.		
15	**Ensure the Use of IMDSv2 is Enforced on All Existing Instances (Manual)** Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled on all running instances.	The IMDSv2 method uses session-based controls to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. With IMDSv2, controls can be implemented to restrict changes to instance metadata.		
16	**Ensure use of AWS Systems Manager to manage EC2 instances (Manual)** An inventory and management of Amazon Elastic Compute Cloud (Amazon EC2) instances is made possible with AWS Systems Manager.	Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment.		
17	**Ensure unused ENIs are removed (Manual)** Identify and delete any unused Amazon AWS Elastic Network Interfaces in order to adhere to best practices and to avoid reaching the service limit. An AWS Elastic Network Interface (ENI) is pronounced unused when is not attached anymore to an EC2 instance.			
18	**Ensure instances stopped for over 90 days are removed (Manual)** Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards.			
19	**Ensure EBS volumes attached to an EC2 instance is marked for deletion upon instance termination (Manual)** This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality.			
20	**Ensure Secrets and Sensitive Data are not stored directly in EC2 User Data (Manual)** User Data can be specified when launching an ec2 instance. Examples include specifying parameters for configuring the instance or including a simple script.	The user data is not protected by authentication or cryptographic methods. Therefore, sensitive data, such as passwords or long-lived encryption keys should not be stored as user data.		
21	**Ensure EC2 Auto Scaling Groups Propagate Tags to EC2 Instances that it launches (Automated)** Tags can help with managing, identifying, organizing, searching for, and filtering resources. Additionally, tags can help with security and compliance. Tags can be propagated from an Auto Scaling group to the EC2 instances that it launches.	Without tags, EC2 instances created via Auto Scaling can be without tags and could be out of compliance with security policy.		

Sr. No	Control	Risk	Status	Auditors Remarks
22	**Apply updates to any apps running in Lightsail (Manual)** Amazon Lightsail is a virtual private server (VPS) provider and is the easiest way to get started with AWS for developers, small businesses, students, and other users who need a solution to build and host their applications on cloud.	Lightsail offers a range of operating system and application templates that are automatically installed when you create a new Lightsail instance. Application templates include WordPress, Drupal, Joomla!, Ghost, Magento, Redmine, LAMP, Nginx (LEMP), MEAN, Node.js, Django, and more. You can install additional software on your instances by using the in-browser SSH or your own SSH client.		
23	**Change default Administrator login names and passwords for applications (Manual)** Change the default settings for the administrator login names and passwords of the application software that you install on Lightsail instances.	Default administrator login names and passwords for applications used on Lightsail instances can be used by hackers and individuals to break into your servers.		
24	**Disable SSH and RDP ports for Lightsail instances when not needed. (Manual)** Any ports enable within Lightsail by default are open and exposed to the world. For SSH and RDP access you should remove and disable these ports when not is use.	Any ports enable within Lightsail by default are open and exposed to the world. This can result in outside traffic trying to access or even deny access to the Lightsail instances. Removing and disabling a protocol when not in use even if restricted by IP address is the safest solution especially when it is not required for access.		
25	**Ensure SSH is restricted to only IP address that should have this access. (Manual)** Any ports enable within Lightsail by default are open and exposed to the world. For SSH and RDP access you should identify which IP address need access.	Any ports enable within Lightsail by default are open and exposed to the world. This can result in outside traffic trying to access or even deny access to the Lightsail instances. Removing and adding approved IP address required for access.		
26	**Ensure RDP is restricted to only IP address that should have this access. (Manual)** Any ports enable within Lightsail by default are open and exposed to the world. For SSH and RDP access you should identify which IP address need access.	Any ports enable within Lightsail by default are open and exposed to the world. This can result in outside traffic trying to access or even deny access to the Lightsail instances. Removing and adding approved IP address required for access.		
27	**Disable IPv6 Networking if not in use within your organization. (Manual)** Any protocols enable within Lightsail by default that aren't being used should be disabled.	Any ports enable within Lightsail by default are open and exposed to the world. This can result in outside traffic trying to access or even deny access to the Lightsail instances. Removing and disabling a protocol when not in use even if restricted by IP address is the safest solution especially when it is not required for access.		
28	**Ensure you are using an IAM policy to manage access to buckets in Lightsail. (Manual)** The following policy grants a user access to manage a specific bucket in the Amazon Lightsail object storage service.	This policy grants access to buckets through the Lightsail console, the AWS Command Line Interface (AWS CLI), AWS API, and AWS SDKs.		
29	**Ensure Lightsail instances are attached to the buckets (Manual)** Attaching an Amazon Lightsail instance to a Lightsail storage bucket gives it full programmatic access to the bucket and its objects.	When you attach instances to buckets, you don't have to manage credentials like access keys. Resource access is ideal if you're configuring software or a plugin on your instance to upload files directly to your bucket. For example, if you want to configure a WordPress instance to store media files on a bucket configuration with bucket storage resource access allows for that securely.		
30	**Ensure that your Lightsail buckets are not publicly accessible (Manual)** You can make all objects private, public (read-only) or private while making individual objects public (read-only). By default when creating a bucket the permissions are set to "All objects are private".	When the Bucket access permissions are set to All objects are public (read-only) – All objects in the bucket are readable by anyone on the internet through the URL of the bucket.		

Sr. No	Control	Risk	Status	Auditors Remarks
31	**Enable storage bucket access logging (Manual)** Access logging provides detailed records for the requests that are made to this bucket. This information can include the request type, the resources that are specified in the request, and the time and date that the request was processed. Access logs are useful for many applications.	Access log information is useful in security and access audits.		
32	**Ensure your Windows Server based lightsail instances are updated with the latest security patches. (Manual)** Windows server based Lightsail instances are still managed by the consumer and any security updates or patches have to be installed and maintained by the user.	Windows Server-based Lightsail instances need to be updated with the latest security patches so they are not vulnerable to attacks. Be sure your server is configured to download and install updates.		
33	**Change the auto-generated password for Windows based instances. (Manual)** When you create a Windows Server-based instance, Lightsail randomly generates a long password that is hard to guess. You use this password uniquely with your new instance. You can use the default password to connect quickly to your instance using remote desktop (RDP). You are always logged in as the Administrator on your Lightsail instance.	Like any password it should be changed from the default and over time. The randomly generated password can be hard to remember and if anyone gains access to your AWS Lightsail environment they can utilize that to access your instances. For this reason you should change the password to something you can remember.		
34	**Ensure AWS Config is Enabled for Lambda and Serverless (Manual)** With AWS Config, you can track configuration changes to the Lambda functions (including deleted functions), runtime environments, tags, handler name, code size, memory allocation, timeout settings, and concurrency settings, along with Lambda IAM execution role, subnet, and security group associations.	This gives you a holistic view of the Lambda function's lifecycle and enables you to surface that data for potential audit and compliance requirements.		
35	**Ensure Cloudwatch Lambda insights is enabled (Manual)** Ensure that Amazon CloudWatch Lambda Insights is enabled for your Amazon Lambda functions for enhanced monitoring.	Amazon CloudWatch Lambda Insights allows you to monitor, troubleshoot, and optimize your Lambda functions. The service collects system-level metrics and summarizes diagnostic information to help you identify issues with your Lambda functions and resolve them as soon as possible. CloudWatch Lambda Insights collects system-level metrics and emits a single performance log event for every invocation of that Lambda function.		
36	**Ensure AWS Secrets manager is configured and being used by Lambda for databases (Manual)** Lambda functions often have to access a database or other services within your environment.	Credentials used to access databases and other AWS Services need to be managed and regularly rotated to keep access into critical systems secure. Keeping any credentials and manually updating the passwords would be cumbersome, but AWS Secrets Manager allows you to manage and rotate passwords.		
37	**Ensure least privilege is used with Lambda function access (Manual)** Lambda is fully integrated with IAM, allowing you to control precisely what each Lambda function can do within the AWS Cloud. As you develop a Lambda function, you expand the scope of this policy to enable access to other resources. For example, for a function that processes objects put into an S3 bucket, it requires read access to objects stored in that bucket. Do not grant the function broader permissions to write or delete data, or operate in other buckets.	You can use AWS Identity and Access Management (IAM) to manage access to the Lambda API and resources like functions and layers. For users and applications in your account that use Lambda, you manage permissions in a permissions policy that you can apply to IAM users, groups, or roles. To grant permissions to other accounts or AWS services that use your Lambda resources, you use a policy that applies to the resource itself.		

Sr. No	Control	Risk	Status	Auditors Remarks
38	**Ensure every Lambda function has its own IAM Role (Manual)** Every Lambda function should have a one to one IAM execution role and the roles should not be shared between functions.	The Principle of Least Privilege means that any Lambda function should have the minimal amount of access required to perform its tasks. In order to accomplish this Lambda functions should not share IAM Execution roles.		
39	**Ensure Lambda functions are not exposed to everyone. (Manual)** A publicly accessible Amazon Lambda function is open to the public and can be reviewed by anyone. To protect against unauthorized users that are sending requests to invoke these functions they need to be changed so they are not exposed to the public.	Allowing anyone to invoke and run your Amazon Lambda functions can lead to data exposure, data loss, and unexpected charges on your AWS bill.		
40	**Ensure Lambda functions are referencing active execution roles. (Manual)** In order to have the necessary permissions to access the AWS cloud services and resources Amazon Lambda functions should be associated with active(available) execution roles.	A Lambda function's execution role is an Identity and Access Management (IAM) role that grants the function permission to process and access specific AWS services and resources. When Amazon Lambda functions are not referencing active execution roles, the functions are losing the ability to perform critical operations securely.		
41	**Ensure that Code Signing is enabled for Lambda functions. (Manual)** Ensure that all your Amazon Lambda functions are configured to use the Code Signing feature in order to restrict the deployment of unverified code.	Code Signing, ensures that the function code is signed by an approved (trusted) source, and that it has not been altered since signing, and that the code signature has not expired or been revoked.		
42	**Ensure there are no Lambda functions with admin privileges within your AWS account (Manual)** Ensure that your Amazon Lambda functions don't have administrative permissions potentially giving the function access to all AWS cloud services and resources.	In order to promote the Principle of Least Privilege (POLP) and provide your functions the minimal amount of access required to perform their tasks the right IAM execution role associated with the function should be used. Instead of providing administrative permissions you should grant the role the necessary permissions that the function really needs.		
43	**Ensure Lambda functions do not allow unknown cross account access via permission policies. (Manual)** Ensure that all your Amazon Lambda functions are configured to allow access only to trusted AWS accounts in order to protect against unauthorized cross-account access.	Allowing unknown (unauthorized) AWS accounts to invoke your Amazon Lambda functions can lead to data exposure and data loss. To prevent any unauthorized invocation requests for your Lambda functions, restrict access only to trusted AWS accounts.		
44	**Ensure that the runtime environment versions used for your Lambda functions do not have end of support dates. (Manual)** Always using a recent version of the execution environment configured for your Amazon Lambda functions adheres to best practices for the newest software features, the latest security patches and bug fixes, and performance and reliability.	When you execute your Lambda functions using recent versions of the implemented runtime environment, you should benefit from new features and enhancements, better security, along with performance and reliability.		
45	**Ensure encryption in transit is enabled for Lambda environment variables (Manual)** As you can set your own environmental variables for Lambda it is important to also encrypt them for in transit protection.	Lambda environment variables should be encrypted in transit for client-side protection as they can store sensitive information.		
46	**Ensure AWS Batch is configured with AWS Cloudwatch Logs. (Manual)** You can configure Batch jobs to send log information to CloudWatch Logs.	This enables you to view different logs from all your jobs in one convenient location.		

Sr. No	Control	Risk	Status	Auditors Remarks
47	**Ensure Batch roles are configured for cross-service confused deputy prevention (Manual)** The Cross-service confused deputy problem is a security issue where an entity that doesn't have permission to perform an action can coerce a more-privileged entity to perform the action.	Cross-service impersonation can result in the confused deputy problem. Cross-service impersonation can occur when one service (the calling service) calls another service (the called service). The calling service can be manipulated to use its permissions to act on another customer's resources in a way it should not otherwise have permission to access.		
48	**Ensure Managed Platform updates is configured (Manual)** AWS Elastic Beanstalk regularly releases platform updates to provide fixes, software updates, and new features. With managed platform updates, you can configure your environment to automatically upgrade to the latest version of a platform during a scheduled maintenance window.	Your application remains in service during the update process with no reduction in capacity. Managed updates are available on both single-instance and load-balanced environments. They also ensure you aren't introducing any vulnerabilities by running legacy systems that require updates and patches.		
49	**Ensure Persistent logs is setup and configured to S3 (Manual)** Elastic Beanstalk can be configured to automatically stream logs to the CloudWatch service.	With CloudWatch Logs, you can monitor and archive your Elastic Beanstalk application, system, and custom log files from Amazon EC2 instances of your environments.		
50	**Ensure access logs are enabled. (Manual)** When you enable load balancing, your AWS Elastic Beanstalk environment is equipped with an Elastic Load Balancing load balancer to distribute traffic among the instances in your environment	For security reasons it is important to have a record of all the access logs and this is enabled within the Load Balancer assigned to the Elastic Beanstalk environments.		
51	**Ensure that HTTPS is enabled on load balancer (Manual)** **T**he simplest way to use HTTPS with an Elastic Beanstalk environment is to assign a server certificate to your environment's load balancer.	When you configure your load balancer to terminate HTTPS, the connection between the client and the load balancer is secure.		
52	**Ensure you are using VPC Endpoints for source code access (Manual)** App Runner needs access to your application source, so it can't be encrypted. Therefore, be sure to secure the connection between your development or deployment environment and App Runner.	Client-side encryption isn't a valid method for protecting the source image or code that you provide to App Runner for deployment. Using a VPC endpoint, you can privately connect your VPC to supported AWS services and VPC endpoint services that are powered by AWS PrivateLink.		
53	**Ensure communications between your applications and clients is encrypted. (Manual)** SimSpace Weaver doesn't manage communications between your apps and the clients.	Be sure to implement some form of authentication and encryption for all client sessions while using SimSpace Weaver.		