# AWS Security Review Checklist

BhanuReddy.cloud | Cloud Security Consulting

## IAM

[ ] IAM users access keys should be rotated every 90 days or less.

[ ] IAM customer-managed policies that you create should not allow wildcard actions for services.

[ ] IAM root user access key should not exist.

[ ] IAM policies should not allow full * administrative privileges.

[ ] MFA should be enabled for all IAM users that have a console password.

[ ] Password policies for IAM users should have strong configurations.

[ ] Unused IAM user credentials should be removed.

[ ] IAM users should not have IAM policies attached.

AWS Security Review Checklist

## EC2

[ ] EC2 instances should not have a public IPv4 address.
[ ] EC2 instances should use Instance Metadata Service Version 2 (IMDSv2).
[ ] Security groups should only allow unrestricted incoming traffic for authorized ports.
[ ] The attached EBS volumes should be encrypted at rest.
[ ] Stopped EC2 instances should be removed after a specified time period.
[ ] Both VPN tunnels for an AWS Site-to-Site VPN connection should be up.
[ ] Network ACLs should not allow ingress from 0.0.0.0/0 to port 22 or port 80.
[ ] EBS snapshots should not be publicly restorable.
[ ] Security groups should not allow unrestricted access to ports with high risk.
[ ] The VPC default security group should not allow inbound and outbound traffic.
[ ] Amazon EC2 should be configured to use VPC endpoints that are created for the Amazon EC2 service.
[ ] EC2 subnets should not automatically assign public IP addresses.
[ ] Unused EC2 security groups should be removed.
[ ] VPC flow logging should be enabled in all VPCs.
[ ] EBS default encryption should be enabled.
[ ] Unused Network Access Control Lists should be removed.
[ ] EC2 instances should not use multiple ENIs.

AWS Security Review Checklist

## S3

[ ] S3 Block Public Access setting should be enabled at the bucket level.
[ ] S3 buckets should have event notifications enabled.
[ ] S3 buckets should require requests to use the Secure Socket Layer.
[ ] S3 access control lists (ACLs) should not be used to manage user access to buckets.
[ ] S3 buckets should prohibit public read access.
[ ] S3 buckets should prohibit public write access.
[ ] S3 buckets with versioning enabled should have lifecycle policies configured.
[ ] S3 buckets should have server-side encryption enabled.
[ ] S3 bucket server access logging should be enabled.
[ ] S3 buckets should have lifecycle policies configured.

## ECR

[ ] ECR private repositories should have image scanning configured.
[ ] ECR private repositories should have tag immutability configured.
[ ] ECR repositories should have at least one lifecycle policy configured.

## RDS

[ ] RDS DB instances should have deletion protection enabled.
[ ] Enhanced monitoring should be configured for RDS DB instances.
[ ] RDS DB instances should be configured to copy tags to snapshots.
[ ] RDS DB clusters should be configured to copy tags to snapshots.
[ ] Database logging should be enabled.
[ ] RDS DB instances should have encryption at rest enabled.
[ ] RDS Database Clusters should use a custom administrator username.
[ ] RDS instances should have automatic backups enabled.
[ ] RDS cluster snapshots and database snapshots should be encrypted at rest.
[ ] RDS instances should not use a database engine default port.
[ ] RDS database instances should use a custom administrator username.
[ ] IAM authentication should be configured for RDS instances.

## OpenSearch / Elasticsearch

[ ] Elasticsearch domains should have audit logging enabled.

[ ] Connections to Elasticsearch domains should be encrypted using TLS 1.2.

[ ] Elasticsearch domains should have encryption at rest enabled.

[ ] Elasticsearch domains should encrypt data sent between nodes.

[ ] Elasticsearch domains should be in a VPC.

[ ] Elasticsearch domain error logging to CloudWatch Logs should be enabled.