# Amazon Web Services Cyber Risk Report

# AWS Cyber Risk Summary

The purpose of this report is to aggregate and summarize information gathered via the AWS SecurityHub service which implements active scaning and testing of an organizations AWS account configuration with a variety of cyber security standards and recommended best practices. This section summarizes information from these active measurements and audits. Each security standard needs to be enabled in each actively used region of AWS. Each standard describes a set of specific controls against specific AWS services or resources. Each control is also associated with a pre determined severity level that captures the importance of that control.

#### Enabled controls for each standard by region

The table below shows how many of the total number of controls in each standard have been enabled for automated testing. User may disable tests or controls that are not relevant to their environment.

Region	CIS AWS Foundations Benchmark v1.2.0	AWS Foundational Security Best Practices v1.0.0	PCI DSS v3.2.1
us-east-1	43/43	93/93	44/44
us-east-2	42/43	87/88	44/44
us-west-2	43/43	88/88	

Total number of passed versus failed controls The chart below represents the relative number of tests that passed versus tests that failed across all standards, regardless of their importance or criticality.



# AWS Foundational Security Best Practices v1.0.0

The AWS Foundational Security Best Practices standard focuses on describing a set of key best practices that users of AWS are expected to adopt for a secure operational environment. These controls span a wide range of AWS services and help an organization improve their security posture while utilizing cloud based AWS services. Each control is associated with a severity label that highlights how critical the best practice described in that control is.



### Findings status by region The chart below shows the status of the findings for this security standard by AWS region



Evaluated asset classes by region The chart below shows the number of findings for different categories of AWS assets for each region

AwsAccount AwsLambdaFunction AwsS3Bucket AwsEc2SecurityGroup AwsCertificateManagerCertificate AwsEc2Vpc AwsDynamoDBTable AwsEc2NetworkAcl AwsElbv2LoadBalancer AwsEc2Subnet AwsEc2Instance 10 20 30 40 50 0 60

us-east-2 us-west-2 us-east-1

#### Controls

The table below presents a summary of the status of each control in this security standard and its status for each region in which it was evaluated. Some controls are evaluated multiple times for multiple assets

Control	us-east-1	us-east-2	us-west-2
ACM.1 ACM certificates should be renewed after a specified time period		PASSED	
AutoScaling.1 Auto scaling groups associated with a load balancer should use load balancer health checks		PASSED	
CloudTrail.2 CloudTrail should have encryption at-rest enabled		PASSED	
CloudTrail.4 CloudTrail log file validation should be enabled		PASSED	
CloudTrail.5 CloudTrail trails should be integrated with Amazon CloudWatch Logs		PASSED	
Cade Duild 1 Cade Duild Cithlub ar Dithugkat agurag rangaitany UDLa chauld use OAuth			
CodeBuild. I CodeBuild GITHUD of BILDUCKET Source repository ORLS should use OAuth		PASSED	
CodeBuild.2 CodeBuild project environment variables should not contain clear text credentials		PASSED	
Config 1 AWS Config should be enabled			
DMS.1 Database Migration Service replication instances should not be public		PASSED	
DynamoDB.1 DynamoDB tables should automatically scale capacity with demand		FAILED	
		TAILED	
DynamoDB.3 DynamoDB Accelerator (DAX) clusters should be encrypted at rest		PASSED	
EC2.1 EBS snapshots should not be public, determined by the ability to be restorable by anyone		PASSED	
EC2.10 Amazon EC2 should be configured to use VPC endpoints		FAILED	
EC2.15 EC2 subnets should not automatically assign public IP addresses		FAILED	
EC2.16 Unused Network Access Control Lists should be removed		FAILED	
EC2.2 The VPC default security group should not allow inbound and outbound traffic		FAILED	
EC2.4 Stopped EC2 instances should be removed after a specified time period		PASSED	
EC2.6 VPC flow logging should be enabled in all VPCs		FAILED	
EC2.7 EBC default apartmetion abould be apabled			
EC2.7 EBS default encryption should be enabled		FAILED	
EFS.1 Elastic File System should be configured to encrypt file data at-rest using AWS KMS		PASSED	
FES 2 Amazon FES volumes should be in backup plans		DASCED	
Er olz Amazon Er o volumes should be in backup pians		PASSED	
ELB.3 Classic Load Balancer listeners should be configured with HTTPS or TLS termination		PASSED	
FLB.4 Application load balancer should be configured to drop bttp boodors		EALLED	
		FAILED	
ELB.5 Application and Classic Load Balancers logging should be enabled		FAILED	
ELB.6 Application Load Balancer deletion protection should be enabled		FAILED	
ELBv2.1 Application Load Balancer should be configured to redirect all HTTP requests to HTTPS		PASSED	
EMR.1 Amazon Elastic MapReduce cluster master nodes should not have public IP addresses		PASSED	
ES.1 Elasticsearch domains should have encryption at-rest enabled		PASSED	
ES.2 Amazon Elasticsearch Service domains should be in a VPC		PASSED	
ES.3 Amazon Elasticsearch domains should encrypt data sent between nodes		PASSED	
ElasticBeanstalk.1 Elastic Beanstalk environments should have enhanced health reporting enabled		PASSED	
ElasticBeanstalk.2 Elastic Beanstalk managed platform updates should be enabled		PASSED	
GuardDuty.1 GuardDuty should be enabled		FAILED	
IAM.1 IAM policies should not allow full "*" administrative privileges		PASSED	
IAM.2 IAM users should not have IAM policies attached		PASSED	
IAM.3 IAM users' access keys should be rotated every 90 days or less		PASSED	
IAM.4 IAM root user access key should not exist		PASSED	
IAM 5 MEA should be enabled for all IAM users that have a console password		DASSED	
IAM.5 MFA should be enabled for all IAM users that have a console password		PASSED	
IAM.5 MFA should be enabled for all IAM users that have a console password IAM.6 Hardware MFA should be enabled for the root user		PASSED FAILED	
IAM.5 MFA should be enabled for all IAM users that have a console password IAM.6 Hardware MFA should be enabled for the root user		PASSED FAILED	
IAM.5 MFA should be enabled for all IAM users that have a console password IAM.6 Hardware MFA should be enabled for the root user IAM.7 Password policies for IAM users should have strong configurations		PASSED FAILED FAILED	
IAM.5 MFA should be enabled for all IAM users that have a console password         IAM.6 Hardware MFA should be enabled for the root user         IAM.7 Password policies for IAM users should have strong configurations         IAM.8 Unused IAM user credentials should be removed		PASSED FAILED FAILED PASSED	
IAM.5 MFA should be enabled for all IAM users that have a console password IAM.6 Hardware MFA should be enabled for the root user IAM.7 Password policies for IAM users should have strong configurations IAM.8 Unused IAM user credentials should be removed KMS.1 IAM customer managed policies should not allow decryption actions on all KMS keys		PASSED FAILED FAILED PASSED PASSED	
IAM.5 MFA should be enabled for all IAM users that have a console password IAM.6 Hardware MFA should be enabled for the root user IAM.7 Password policies for IAM users should have strong configurations IAM.8 Unused IAM user credentials should be removed KMS.1 IAM customer managed policies should not allow decryption actions on all KMS keys		PASSED FAILED FAILED PASSED PASSED	
IAM.5 MFA should be enabled for all IAM users that have a console passwordIAM.6 Hardware MFA should be enabled for the root userIAM.7 Password policies for IAM users should have strong configurationsIAM.8 Unused IAM user credentials should be removedKMS.1 IAM customer managed policies should not allow decryption actions on all KMS keysKMS.2 IAM principals should not have IAM inline policies that allow decryption actions on all KMS keys		PASSED FAILED FAILED PASSED PASSED PASSED	
IAM.5 MFA should be enabled for all IAM users that have a console password         IAM.6 Hardware MFA should be enabled for the root user         IAM.7 Password policies for IAM users should have strong configurations         IAM.8 Unused IAM user credentials should be removed         KMS.1 IAM customer managed policies should not allow decryption actions on all KMS keys         KMS.2 IAM principals should not have IAM inline policies that allow decryption actions on all KMS keys         KMS.3 AWS KMS keys should not be deleted unintentionally		PASSED FAILED FAILED PASSED PASSED PASSED	
IAM.5 MFA should be enabled for all IAM users that have a console password IAM.6 Hardware MFA should be enabled for the root user IAM.7 Password policies for IAM users should have strong configurations IAM.8 Unused IAM user credentials should be removed KMS.1 IAM customer managed policies should not allow decryption actions on all KMS keys KMS.2 IAM principals should not have IAM inline policies that allow decryption actions on all KMS keys KMS.3 AWS KMS keys should not be deleted unintentionally		PASSED FAILED FAILED PASSED PASSED PASSED PASSED	
IAM.5 MFA should be enabled for all IAM users that have a console passwordIAM.6 Hardware MFA should be enabled for the root userIAM.7 Password policies for IAM users should have strong configurationsIAM.8 Unused IAM user credentials should be removedKMS.1 IAM customer managed policies should not allow decryption actions on all KMS keysKMS.2 IAM principals should not have IAM inline policies that allow decryption actions on all KMS keysKMS.3 AWS KMS keys should not be deleted unintentionallyLambda.1 Lambda function policies should prohibit public access		PASSED FAILED FAILED PASSED PASSED PASSED PASSED PASSED	
IAM.5 MFA should be enabled for all IAM users that have a console password         IAM.6 Hardware MFA should be enabled for the root user         IAM.7 Password policies for IAM users should have strong configurations         IAM.8 Unused IAM user credentials should be removed         KMS.1 IAM customer managed policies should not allow decryption actions on all KMS keys         KMS.2 IAM principals should not have IAM inline policies that allow decryption actions on all KMS keys         KMS.3 AWS KMS keys should not be deleted unintentionally         Lambda.1 Lambda function policies should use supported runtimes		PASSED FAILED FAILED PASSED PASSED PASSED PASSED PASSED	
IAM.5 MFA should be enabled for all IAM users that have a console password         IAM.6 Hardware MFA should be enabled for the root user         IAM.7 Password policies for IAM users should have strong configurations         IAM.8 Unused IAM user credentials should be removed         KMS.1 IAM customer managed policies should not allow decryption actions on all KMS keys         KMS.2 IAM principals should not have IAM inline policies that allow decryption actions on all KMS keys         KMS.3 AWS KMS keys should not be deleted unintentionally         Lambda.1 Lambda function policies should use supported runtimes		PASSED FAILED FAILED PASSED PASSED PASSED PASSED PASSED	
IAM.5 MFA should be enabled for all IAM users that have a console password         IAM.6 Hardware MFA should be enabled for the root user         IAM.7 Password policies for IAM users should have strong configurations         IAM.8 Unused IAM user credentials should be removed         KMS.1 IAM customer managed policies should not allow decryption actions on all KMS keys         KMS.2 IAM principals should not have IAM inline policies that allow decryption actions on all KMS keys         KMS.3 AWS KMS keys should not be deleted unintentionally         Lambda.1 Lambda function policies should use supported runtimes         Lambda.4 Lambda functions should have a dead-letter queue configured		PASSED FAILED FAILED PASSED PASSED PASSED PASSED PASSED PASSED FAILED	
IAM.5 MFA should be enabled for all IAM users that have a console password         IAM.6 Hardware MFA should be enabled for the root user         IAM.7 Password policies for IAM users should have strong configurations         IAM.8 Unused IAM user credentials should be removed         KMS.1 IAM customer managed policies should not allow decryption actions on all KMS keys         KMS.2 IAM principals should not have IAM inline policies that allow decryption actions on all KMS keys         KMS.3 AWS KMS keys should not be deleted unintentionally         Lambda.1 Lambda function policies should prohibit public access         Lambda.4 Lambda functions should have a dead-letter queue configured         RDS.1 RDS snapshot should be private		PASSED FAILED FAILED PASSED PASSED PASSED PASSED PASSED FAILED PASSED	
IAM.5 MFA should be enabled for all IAM users that have a console password         IAM.6 Hardware MFA should be enabled for the root user         IAM.7 Password policies for IAM users should have strong configurations         IAM.8 Unused IAM user credentials should be removed         KMS.1 IAM customer managed policies should not allow decryption actions on all KMS keys         KMS.2 IAM principals should not have IAM inline policies that allow decryption actions on all KMS keys         KMS.3 AWS KMS keys should not be deleted unintentionally         Lambda.1 Lambda function policies should prohibit public access         Lambda.4 Lambda functions should have a dead-letter queue configured         RDS.1 RDS snapshot should be private         PDC 40 MM suther time time the policies of the configured		PASSED FAILED FAILED PASSED PASSED PASSED PASSED PASSED FAILED FAILED	
IAM.5 MFA should be enabled for all IAM users that have a console passwordIAM.6 Hardware MFA should be enabled for the root userIAM.7 Password policies for IAM users should have strong configurationsIAM.8 Unused IAM user credentials should be removedKMS.1 IAM customer managed policies should not allow decryption actions on all KMS keysKMS.2 IAM principals should not have IAM inline policies that allow decryption actions on all KMS keysKMS.3 AWS KMS keys should not be deleted unintentionallyLambda.1 Lambda function policies should prohibit public accessLambda.2 Lambda functions should have a dead-letter queue configuredRDS.1 RDS snapshot should be privateRDS.10 IAM authentication should be configured for RDS instances		PASSED FAILED FAILED PASSED PASSED PASSED PASSED PASSED FAILED FAILED PASSED	
IAM.5 MFA should be enabled for all IAM users that have a console password         IAM.6 Hardware MFA should be enabled for the root user         IAM.7 Password policies for IAM users should have strong configurations         IAM.8 Unused IAM user credentials should be removed         KMS.1 IAM customer managed policies should not allow decryption actions on all KMS keys         KMS.2 IAM principals should not have IAM inline policies that allow decryption actions on all KMS keys         KMS.3 AWS KMS keys should not be deleted unintentionally         Lambda.1 Lambda function policies should prohibit public access         Lambda.4 Lambda functions should have a dead-letter queue configured         RDS.10 IAM authentication should be configured for RDS instances         RDS.12 IAM authentication should be configured for RDS clusters		PASSED FAILED FAILED PASSED PASSED PASSED PASSED FAILED PASSED PASSED PASSED	
IAM.5 MFA should be enabled for all IAM users that have a console password         IAM.6 Hardware MFA should be enabled for the root user         IAM.7 Password policies for IAM users should have strong configurations         IAM.8 Unused IAM user credentials should be removed         KMS.1 IAM customer managed policies should not allow decryption actions on all KMS keys         KMS.2 IAM principals should not have IAM inline policies that allow decryption actions on all KMS keys         KMS.3 AWS KMS keys should not be deleted unintentionally         Lambda.1 Lambda function policies should prohibit public access         Lambda.2 Lambda functions should have a dead-letter queue configured         RDS.10 IAM authentication should be configured for RDS instances         RDS.12 IAM authentication should be configured for RDS clusters         PDS 13 PDS automatic miner unregion underedies should be centricit		PASSED FAILED FAILED PASSED PASSED PASSED PASSED FAILED FAILED PASSED PASSED PASSED	
IAM.5 MFA should be enabled for all IAM users that have a console password         IAM.6 Hardware MFA should be enabled for the root user         IAM.7 Password policies for IAM users should have strong configurations         IAM.8 Unused IAM user credentials should be removed         KMS.1 IAM customer managed policies should not allow decryption actions on all KMS keys         KMS.2 IAM principals should not have IAM inline policies that allow decryption actions on all KMS keys         KMS.3 AWS KMS keys should not be deleted unintentionally         Lambda.1 Lambda function policies should prohibit public access         Lambda.2 Lambda functions should have a dead-letter queue configured         RDS.1 RDS snapshot should be private         RDS.10 IAM authentication should be configured for RDS instances         RDS.13 RDS automatic minor version upgrades should be enabled		PASSED FAILED FAILED PASSED PASSED PASSED PASSED FAILED FAILED PASSED PASSED PASSED PASSED	
IAM.5 MFA should be enabled for all IAM users that have a console password         IAM.6 Hardware MFA should be enabled for the root user         IAM.7 Password policies for IAM users should have strong configurations         IAM.8 Unused IAM user credentials should be removed         KMS.1 IAM customer managed policies should not allow decryption actions on all KMS keys         KMS.2 IAM principals should not have IAM inline policies that allow decryption actions on all KMS keys         KMS.3 AWS KMS keys should not be deleted unintentionally         Lambda.1 Lambda function policies should prohibit public access         Lambda.2 Lambda functions should have a dead-letter queue configured         RDS.10 IAM authentication should be configured for RDS instances         RDS.10 IAM authentication should be configured for RDS clusters         RDS.13 RDS automatic minor version upgrades should be enabled         RDS.13 RDS automatic minor version upgrades should be enabled		PASSED FAILED FAILED PASSED PASSED PASSED PASSED FAILED PASSED PASSED PASSED PASSED PASSED PASSED	
IAM.5 MFA should be enabled for all IAM users that have a console password         IAM.6 Hardware MFA should be enabled for the root user         IAM.7 Password policies for IAM users should have strong configurations         IAM.8 Unused IAM user credentials should be removed         KMS.1 IAM customer managed policies should not allow decryption actions on all KMS keys         KMS.2 IAM principals should not have IAM inline policies that allow decryption actions on all KMS keys         KMS.3 AWS KMS keys should not be deleted unintentionally         Lambda.1 Lambda function policies should prohibit public access         Lambda.2 Lambda functions should have a dead-letter queue configured         RDS.10 IAM authentication should be configured for RDS instances         RDS.11 IAM authentication should be configured for RDS clusters         RDS.13 RDS automatic minor version upgrades should be enabled         RDS.13 RDS DB Instances should prohibit public access.         RDS.14 Amazon Aurora clusters should have backtracking enabled         RDS.2 RDS DB Instances should prohibit public access.		PASSED FAILED FAILED PASSED PASSED PASSED PASSED FAILED FAILED PASSED PASSED PASSED PASSED PASSED PASSED	
IAM.5 MFA should be enabled for all IAM users that have a console password         IAM.6 Hardware MFA should be enabled for the root user         IAM.7 Password policies for IAM users should have strong configurations         IAM.8 Unused IAM user credentials should be removed         KMS.1 IAM customer managed policies should not allow decryption actions on all KMS keys         KMS.2 IAM principals should not have IAM inline policies that allow decryption actions on all KMS keys         KMS.3 AWS KMS keys should not be deleted unintentionally         Lambda.1 Lambda function policies should prohibit public access         Lambda.2 Lambda functions should use supported runtimes         Lambda.4 Lambda functions should be configured for RDS instances         RDS.10 IAM authentication should be configured for RDS clusters         RDS.13 RDS automatic minor version upgrades should be enabled         RDS.13 RDS automatic minor version upgrades should be enabled         RDS.2 RDS DB Instances should prohibit public access, determined by the PubliclyAccessible configuration		PASSED FAILED FAILED PASSED PASSED PASSED PASSED PASSED FAILED PASSED PASSED PASSED PASSED PASSED PASSED PASSED	
IAM.5 MFA should be enabled for all IAM users that have a console password         IAM.6 Hardware MFA should be enabled for the root user         IAM.7 Password policies for IAM users should have strong configurations         IAM.8 Unused IAM user credentials should be removed         KMS.1 IAM customer managed policies should not allow decryption actions on all KMS keys         KMS.2 IAM principals should not have IAM inline policies that allow decryption actions on all KMS keys         KMS.3 AWS KMS keys should not be deleted unintentionally         Lambda.1 Lambda function policies should prohibit public access         Lambda.2 Lambda functions should use supported runtimes         Lambda.4 Lambda functions should be configured for RDS instances         RDS.10 IAM authentication should be configured for RDS clusters         RDS.13 RDS automatic minor version upgrades should be enabled         RDS.2 RDS DB Instances should prohibit public access, determined by the PubliclyAccessible configuration         RDS.2 RDS DB Instances should have backtracking enabled		PASSED FAILED FAILED PASSED PASSED PASSED PASSED FAILED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED	
IAM.5 MFA should be enabled for all IAM users that have a console password         IAM.6 Hardware MFA should be enabled for the root user         IAM.7 Password policies for IAM users should have strong configurations         IAM.8 Unused IAM user credentials should be removed         KMS.1 IAM customer managed policies should not allow decryption actions on all KMS keys         KMS.2 IAM principals should not have IAM inline policies that allow decryption actions on all KMS keys         KMS.3 AWS KMS keys should not be deleted unintentionally         Lambda.1 Lambda function policies should prohibit public access         Lambda.4 Lambda functions should have a dead-letter queue configured         RDS.1 RDS snapshot should be configured for RDS instances         RDS.12 IAM authentication should be configured for RDS clusters         RDS.12 IAM authentication should be configured for RDS clusters         RDS.12 RDS automatic minor version upgrades should be enabled         RDS.2 RDS DB Instances should prohibit public access, determined by the PubliclyAccessible configuration         RDS.2 RDS DB Instances should have encryption at-rest enabled         RDS.4 RDS cluster snapshots and database snapshots should be encrypted at rest		PASSED FAILED FAILED PASSED PASSED PASSED PASSED FAILED FAILED PASSED PASSED PASSED PASSED PASSED PASSED PASSED	
IAM.5 MFA should be enabled for all IAM users that have a console password         IAM.6 Hardware MFA should be enabled for the root user         IAM.7 Password policies for IAM users should have strong configurations         IAM.8 Unused IAM user credentials should be removed         KMS.1 IAM customer managed policies should not allow decryption actions on all KMS keys         KMS.2 IAM principals should not have IAM inline policies that allow decryption actions on all KMS keys         KMS.3 AWS KMS keys should not be deleted unintentionally         Lambda.1 Lambda function policies should prohibit public access         Lambda.4 Lambda functions should have a dead-letter queue configured         RDS.1 RDS snapshot should be configured for RDS clusters         RDS.12 IAM authentication should be configured for RDS clusters         RDS.13 RDS automatic minor version upgrades should be enabled         RDS.2 RDS DB Instances should prohibit public access, determined by the PubliclyAccessible configuration         RDS.2 RDS DB Instances should have encryption at-rest enabled         RDS.4 RDS cluster snapshots and database enapshots should be encrypted at rest		PASSED FAILED FAILED PASSED PASSED PASSED PASSED PASSED FAILED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED	
IAM.5 MFA should be enabled for all IAM users that have a console password         IAM.6 Hardware MFA should be enabled for the root user         IAM.7 Password policies for IAM users should have strong configurations         IAM.8 Unused IAM user credentials should be removed         KMS.1 IAM customer managed policies should not allow decryption actions on all KMS keys         KMS.2 IAM principals should not have IAM inline policies that allow decryption actions on all KMS keys         KMS.3 AWS KMS keys should not be deleted unintentionally         Lambda.1 Lambda function policies should prohibit public access         Lambda.2 Lambda functions should use supported runtimes         RDS.10 IAM authentication should be configured for RDS instances         RDS.10 IAM authentication should be configured for RDS clusters         RDS.12 IAM authentication should be configured for RDS clusters         RDS.13 RDS automatic minor version upgrades should be enabled         RDS.2 RDS DB Instances should prohibit public access, determined by the PubliclyAccessible configuration         RDS.14 Amazon Aurora clusters should have backtracking enabled         RDS.2 RDS DB Instances should have encryption at-rest enabled         RDS.3 RDS DB Instances should have encryption at-rest enabled         RDS.4 RDS Cluster snapshots and database snapshots should be encrypted at rest         RDS.4 RDS DB Instances should be configured with multiple Availability Zones		PASSED FAILED FAILED PASSED PASSED PASSED PASSED FAILED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED	
IAM.5 MFA should be enabled for all IAM users that have a console password         IAM.6 Hardware MFA should be enabled for the root user         IAM.7 Password policies for IAM users should have strong configurations         IAM.8 Unused IAM user credentials should be removed         KMS.1 IAM customer managed policies should not allow decryption actions on all KMS keys         KMS.2 IAM principals should not have IAM inline policies that allow decryption actions on all KMS keys         KMS.3 AWS KMS keys should not be deleted unintentionally         Lambda.1 Lambda function policies should prohibit public access         Lambda.4 Lambda functions should use supported runtimes         LAmbda.4 Lambda functions should have a dead-letter queue configured         RDS.11 RDS snapshot should be configured for RDS instances         RDS.12 IAM authentication should be configured for RDS clusters         RDS.13 RDS automatic minor version upgrades should be enabled         RDS.2 RDS DB Instances should prohibit public access, determined by the PubliclyAccessible configuration         RDS.2 RDS DB Instances should prohibit public access, determined by the PubliclyAccessible configuration         RDS.2 RDS DB Instances should have encryption at-rest enabled         RDS.3 RDS DB Instances should have encryption at-rest enabled         RDS.13 RDS automatic minor version upgrades should be encrypted at rest         RDS.2 RDS DB Instances should have encryption at-rest enabled         RDS.4 RDS cluster snapsho		PASSED FAILED FAILED PASSED PASSED PASSED PASSED FAILED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED	
IAM.5 MFA should be enabled for all IAM users that have a console password         IAM.6 Hardware MFA should be enabled for the root user         IAM.7 Password policies for IAM users should have strong configurations         IAM.8 Unused IAM user credentials should be removed         KMS.1 IAM customer managed policies should not allow decryption actions on all KMS keys         KMS.2 IAM principals should not have IAM inline policies that allow decryption actions on all KMS keys         KMS.3 AWS KMS keys should not be deleted unintentionally         Lambda.1 Lambda function policies should prohibit public access         Lambda.4 Lambda functions should use supported runtimes         Lambda.4 Lambda functions should have a dead-letter queue configured         RDS.1 RDS snapshot should be private         RDS.10 IAM authentication should be configured for RDS clusters         RDS.13 RDS automatic minor version upgrades should be enabled         RDS.2 RDS DB Instances should prohibit public access, determined by the PubliclyAccessible configuration         RDS.3 RDS DB Instances should have encryption at-rest enabled         RDS.4 RDS cluster snapshots and database snapshots should be encrypted at rest         RDS.5 RDS DB Instances should be configured for RDS DB Instances         RDS.4 RDS cluster snapshots and database snapshots should be encrypted at rest         RDS.4 RDS cluster snapshots and database snapshots should be encrypted at rest         RDS.5 RDS DB Instances should be configured fo		PASSED FAILED FAILED PASSED PASSED PASSED PASSED FAILED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED	
IAM.5 MFA should be enabled for all IAM users that have a console password         IAM.6 Hardware MFA should be enabled for the root user         IAM.7 Password policies for IAM users should have strong configurations         IAM.8 Unused IAM user credentials should be removed         KMS.1 IAM customer managed policies should not allow decryption actions on all KMS keys         KMS.2 IAM principals should not have IAM inline policies that allow decryption actions on all KMS keys         KMS.2 IAM principals should not be deleted unintentionally         Lambda.1 Lambda function policies should prohibit public access         Lambda.2 Lambda functions should use supported runtimes         Lambda.4 Lambda functions should be configured for RDS instances         RDS.10 IAM authentication should be configured for RDS clusters         RDS.11 IAM authentication should have backtracking enabled         RDS.2 RDS DB Instances should prohibit public access, determined by the PubliclyAccessible configuration         RDS.2 RDS DB Instances should prohibit public access, determined by the PubliclyAccessible configuration         RDS.4 RDS cluster snapshots and database snapshots should be enarypted at rest         RDS.4 RDS DB Instances should prohibit public access, determined by the PubliclyAccessible configuration         RDS.4 RDS cluster snapshots and database snapshots should be encrypted at rest         RDS.4 RDS Cluster snapshots and database snapshots should be encrypted at rest         RDS.5 RDS DB Instances should be config		PASSEDFAILEDFAILEDPASSED	
IAM.5 MFA should be enabled for all IAM users that have a console password         IAM.6 Hardware MFA should be enabled for the root user         IAM.7 Password policies for IAM users should have strong configurations         IAM.8 Unused IAM user credentials should be removed         KMS.1 IAM customer managed policies should not allow decryption actions on all KMS keys         KMS.2 IAM principals should not have IAM inline policies that allow decryption actions on all KMS keys         KMS.3 AWS KMS keys should not be deleted unintentionally         Lambda.1 Lambda function policies should prohibit public access         Lambda.2 Lambda functions should use supported runtimes         Lambda.4 Lambda functions should be configured for RDS instances         RDS.10 IAM authentication should be configured for RDS clusters         RDS.11 IAM authentication should have backtracking enabled         RDS.2 RDS automatic minor version upgrades should be enabled         RDS.2 RDS DB Instances should prohibit public access, determined by the PubliclyAccessible configuration         RDS.4 RDS clusters should have encryption at-rest enabled         RDS.4 RDS cluster snapshots and database snapshots should be encrypted at rest         RDS.4 RDS cluster snapshots and database snapshots should be encrypted at rest         RDS.4 RDS clusters should have encryption at-rest enabled         RDS.4 RDS clusters should be configured for RDS DB Instances         RDS.4 RDS Clusters should be configured for RDS DB Instanc		PASSED FAILED FAILED PASSED PASSED PASSED PASSED FAILED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED	
IAM.5 MFA should be enabled for all IAM users that have a console password         IAM.6 Hardware MFA should be enabled for the root user         IAM.7 Password policies for IAM users should have strong configurations         IAM.8 Unused IAM user credentials should be removed         KMS.11AM customer managed policies should not allow decryption actions on all KMS keys         KMS.2 IAM principals should not have IAM inline policies that allow decryption actions on all KMS keys         KMS.3 AWS KMS keys should not be deleted unintentionally         Lambda.1 Lambda function policies should prohibit public access         Lambda.2 Lambda function should use supported runtimes         Lambda.4 Lambda functions should have a dead-letter queue configured         RDS.11 RDS snapshot should be private         RDS.12 IAM authentication should be configured for RDS instances         RDS.12 IAM authentication should be configured for RDS clusters         RDS.13 RDS automatic minor version upgrades should be enabled         RDS.2 RDS DB Instances should have backtracking enabled         RDS.4 RDS cluster snapshots and database snapshots should be encrypted at rest         RDS.4 RDS cluster snapshots and database snapshots should be encrypted at rest         RDS.4 RDS clusters should have encryption rection enabled         RDS.4 RDS clusters should be configured for RDS DB instances         RDS.4 RDS clusters should be configured with multiple Availability Zones         RDS.4 RDS C		PASSED FAILED FAILED PASSED PASSED PASSED PASSED FAILED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED	
IAM.5 MFA should be enabled for all IAM users that have a console password         IAM.6 Hardware MFA should be enabled for the root user         IAM.7 Password policies for IAM users should have strong configurations         IAM.8 Unused IAM user credentials should be removed         KMS.1 IAM customer managed policies should not allow decryption actions on all KMS keys         KMS.2 IAM principals should not have IAM inline policies that allow decryption actions on all KMS keys         KMS.3 AWS KMS keys should not be deleted unintentionally         Lambda.1 Lambda function policies should prohibit public access         Lambda.2 Lambda functions should use supported runtimes         Lambda.4 Lambda functions should be configured for RDS instances         RDS.10 IAM authentication should be configured for RDS clusters         RDS.11 RDS automatic minor version upgrades should be enabled         RDS.2 RDS DB Instances should have backtracking enabled         RDS.3 RDS DB Instances should have encryption at-rest enabled         RDS.4 RDS cluster snapshots and database snapshots should be encrypted at rest         RDS.4 RDS Cluster snapshot and database snapshots should be ancrypted at rest         RDS.4 RDS cluster should have deletion protection enabled         RDS.4 RDS clusters should be configured for RDS DB instances         RDS.4 RDS cluster snapshots and database snapshots should be encrypted at rest         RDS.5 RDS DB Instances should be configured for RDS DB instances		PASSED FAILED FAILED PASSED PASSED PASSED PASSED FAILED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED	
IAM.5 MFA should be enabled for all IAM users that have a console password         IAM.6 Hardware MFA should be enabled for the root user         IAM.7 Password policies for IAM users should have strong configurations         IAM.8 Unused IAM user credentials should be removed         KMS.1 IAM customer managed policies should not allow decryption actions on all KMS keys         KMS.2 IAM principals should not have IAM inline policies that allow decryption actions on all KMS keys         KMS.3 AWS KMS keys should not be deleted unintentionally         Lambda.1 Lambda functions should not be deleted unintentionally         Lambda.2 Lambda functions should have a dead-letter queue configured         RDS.1 RDS snapshot should be private         RDS.10 IAM authentication should be configured for RDS instances         RDS.12 IAM authentication should be configured for RDS clusters         RDS.13 RDS automatic minor version upgrades should be enabled         RDS.2 RDS DB Instances should have backtracking enabled         RDS.2 RDS DB Instances should have encryption at-rest enabled         RDS.4 RDS clusters should be configured for RDS DB instances         RDS.4 RDS clusters should be configured for RDS DB instances         RDS.4 RDS clusters should have encryption at-rest enabled         RDS.5 RDS DB Instances should be configured for RDS DB instances         RDS.4 RDS clusters should have deletion protection enabled         RDS.5 RDS DB Instances should be configured for RD		PASSEDFAILEDFAILEDPASSED	
IAM.5 MFA should be enabled for all IAM users that have a console password         IAM.6 Hardware MFA should be enabled for the root user         IAM.7 Password policies for IAM users should have strong configurations         IAM.8 Unused IAM user credentials should be removed         KMS.1 IAM customer managed policies should not allow decryption actions on all KMS keys         KMS.2 IAM principals should not have IAM inline policies that allow decryption actions on all KMS keys         KMS.3 AWS KMS keys should not be delated unintentionally         Lambda.1 Lambda function policies should prohibit public access         Lambda.2 Lambda function should use supported runtimes         Lambda.4 Lambda function should be configured for RDS instances         RDS.10 IAM authentication should be configured for RDS clusters         RDS.11 IAM authentication should be configured for RDS clusters         RDS.12 IAM authentication should have access, determined by the PubliclyAccessible configuration         RDS.2 RDS DB Instances should have encryption at-rest enabled         RDS.4 RDS cluster snapshots and database snapshots should be encrypted at rest         RDS.4 RDS DB Instances should be configured for RDS DB Instances         RDS.4 RDS cluster snapshots and database snapshots should be encrypted at rest         RDS.4 RDS DB Instances should have encryption at-rest enabled         RDS.4 RDS DB Instances should be configured for RDS DB Instances         RDS.5 RDS DB Instances should be configured for		PASSED FAILED FAILED PASSED PASSED PASSED PASSED FAILED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED	
IAM.5 MFA should be enabled for all IAM users that have a console password         IAM.6 Hardware MFA should be enabled for the root user         IAM.7 Password policies for IAM users should have strong configurations         IAM.8 Unused IAM user credentials should be removed         KMS.1 IAM customer managed policies should not allow decryption actions on all KMS keys         KMS.2 IAM principals should not have IAM inline policies that allow decryption actions on all KMS keys         KMS.3 AWS KMS keys should not be deleted unintentionally         Lambda.1 Lambda function policies should prohibit public access         Lambda.2 Lambda functions should use supported runtimes         Lambda.4 Lambda functions should be orifigured for RDS clusters         RDS.10 IAM authentication should be configured for RDS clusters         RDS.11 IAM authentication should have backtracking enabled         RDS.12 IAM authentication should have backtracking enabled         RDS.12 IAM authentication should have backtracking enabled         RDS.2 RDS DB Instances should have encryption at-rest enabled         RDS.2 RDS DB Instances should have encryption at-rest enabled         RDS.4 RDS Cluster snapshots and database snapshots should be encrypted at rest         RDS.6 RDS DB Instances should be configured with multiple Availability Zones         RDS.6 RDS DB Instances should be configured with multiple Availability Zones         RDS.6 RDS DB Instances should have deletion protection enabled <tr< td=""><td></td><td>PASSED FAILED FAILED PASSED PASSED PASSED PASSED FAILED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED</td><td></td></tr<>		PASSED FAILED FAILED PASSED PASSED PASSED PASSED FAILED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED	
IAM-5 MRA should be enabled for all IAM users that have a console password           IAM.6 Hardware MRA should be enabled for the root user           IAM.7 Password policies for IAM users should have strong configurations           IAM.8 Unused IAM user credentials should not allow decryption actions on all KMS keys           KMS.1 IAM customer managed policies should not allow decryption actions on all KMS keys           KMS.2 IAM principals should not have IAM inline policies that allow decryption actions on all KMS keys           KMS.3 AWS KMS keys should not be deleted unintentionally           Lambda.1 Lambda function policies should prohibit public access           Lambda.2 Lambda functions should have a dead-letter queue configured           RDS.10 IAM authentication should be configured for RDS instances           RDS.11 IAM authentication should be configured for RDS clusters           RDS.12 IAM authentication should be configured for RDS clusters           RDS.13 RDS automatic minor version upgrades should be enabled           RDS.2 RDS DB Instances should have backtracking enabled           RDS.2 RDS DB Instances should be configured for RDS DB instances           RDS.4 Amazon Aurora clusters should have backtracking enabled           RDS.5 RDS DB Instances should have benryption at-rest enabled           RDS.5 RDS DB Instances should have deletion protection enabled           RDS.5 RDS DB Instances should have deletion protection enabled           RDS.6 Enhanced monitoring should be configur		PASSED FAILED FAILED PASSED PASSED PASSED PASSED FAILED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED	
IAM.5 MRA should be enabled for the root user         IAM.6 Hardware MRA should be enabled for the root user         IAM.7 Password policies for IAM users should have strong configurations         IAM.8 Unused IAM user credentials should not allow decryption actions on all KMS keys         KMS.1 IAM customer managed policies should not allow decryption actions on all KMS keys         KMS.2 IAM principals should not have IAM inline policies that allow decryption actions on all KMS keys         KMS.2 IAM principals should not be deleted unintentionally         Lambda.1 Lambda function policies should prohibit public access         Lambda.2 Lambda functions should use supported runtimes         Lambda.4 Lambda functions should be configured for RDS instances         RDS.10 IAM authentication should be configured for RDS clusters         RDS.12 IAM authentication should have backtracking enabled         RDS.2 RDS DB Instances should have backtracking enabled         RDS.2 RDS DB Instances should have encryption at-rest enabled         RDS.4 RDS cluster snephots and database snapshots should be encrypted at rest         RDS.4 RDS DB Instances should be configured for RDS DB Instances         RDS.4 RDS DB Instances should be configured with multiple Availability Zones         RDS.4 RDS DB Instances should be configured for RDS DB Instances         RDS.5 RDS DB Instances should be configured for RDS DB Instances         RDS.7 RDS Clusters should be configured with multiple Availability Zones </td <td></td> <td>PASSED FAILED FAILED PASSED PASSED PASSED PASSED PASSED FAILED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED</td> <td></td>		PASSED FAILED FAILED PASSED PASSED PASSED PASSED PASSED FAILED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED	
IAM.5 MFA should be enabled for all IAM users that have a console password         IAM.6 Hardware MFA should be onabled for the root user         IAM.7 Password policies for IAM users should have strong configurations         IAM.8 Unused IAM user credentials should have strong configurations         IAM.8 Unused IAM user credentials should not allow decryption actions on all KMS keys         KMS.1 IAM customer managed policies should not allow decryption actions on all KMS keys         KMS.3 AWS KMS keys should not have IAM inline policies that allow decryption actions on all KMS keys         Lambda.1 Lambda function policies should prehibit public access         Lambda.2 Lambda functions should use supported runtimes         Lambda.4 Lambda functions should have a dead-letter queue configured         RDS.10 IAM authentication should be configured for RDS instances         RDS.11 CM authentication should be configured for RDS clusters         RDS.12 IAM authentication should have backtrocking enabled         RDS.22 RDS DB Instances should prohibit public access, determined by the PubliclyAccessible configuration         RDS.24 RDS CDB instances should have backtrocking enabled         RDS.24 RDS DB Instances should have energyption at-rest enabled         RDS.24 RDS DB Instances should have configured for RDS DB Instances         RDS.44 RDS cluster snapshots and database snapshots should be encrypted at rest         RDS.54 RDS DB Instances should have deletion protection enabled         RDS.74 R		PASSED FAILED FAILED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED	
IAM.5 MFA should be enabled for all IAM users that have a console password           IAM.6 Hardware MFA should be enabled for the root user           IAM.7 Password policies for IAM users should have strong configurations           IAM.8 Unused IAM user credentials should be removed           KMS.1 IAM customer managed policies should not allow decryption actions on all KMS keys           KMS.2 IAM principals should not have IAM inline policies that allow decryption actions on all KMS keys           KMS.2 IAM principals should not be deleted unintentionally           Lambda.1 Lambda functions policies should prohibit public access           Lambda.2 Lambda functions should have a dead-letter queue configured           RDS.1 RDS snapshot should be private           RDS.10 IAM authentication should be configured for RDS instances           RDS.12 IAM authentication should be configured for RDS clusters           RDS.13 RDS automatic minor version upgrades should be enabled           RDS.24 RDS DB instances should prohibit public access, determined by the PubliclyAccessible configuration           RDS.24 RDS DB instances should prohibit public access, determined by the PubliclyAccessible configuration           RDS.24 RDS DB instances should have alconfigured for RDS DB instances           RDS.44 RDS clusters snapshots and database snapshots should be encrypted at rest           RDS.47 RDS Clusters snapshots and database snapshots should be encrypted at rest           RDS.47 RDS clusters should have deletion protection enabled		PASSED FAILED FAILED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED	
IAA.5 MFA should be enabled for all IAM users that have a console password           IAA.6 Hardware MFA should be enabled for the root user           IAA.7 Password policies for IAM users should have strong configurations           IAM.8 Unused IAM user credentials should be removed           KMS.1 IAM customer managed policies should not allow decryption actions on all KMS keys           KMS.2 IAM principals should not have IAM inline policies that allow decryption actions on all KMS keys           KMS.3 AWS KMS keys should not be deleted unintentionally           Lambda.1 Lambda function policies should prohibit public access           Lambda.2 Lambda functions should use supported runtimes           Lambda.4 Lambda function should have a dead-letter queue configured           RDS.10 IAM authentication should be configured for RDS instances           RDS.10 IAM authentication should be configured for RDS clusters           RDS.11 RDS automatic minor version upgrades should be enabled           RDS.12 IAM authentication should prohibit public access, determined by the PubliclyAccessible configuration           RDS.24 RDS DB Instances should have acternigured for RDS DB instances           RDS.37 RDS abl instances should have encryption at-rest enabled           RDS.47 RDS Clusters should have deletion protection enabled           RDS.57 RDS DB Instances should have deletion protection enabled           RDS.58 RDS DB Instances should have deletion protection enabled           RDS.59 DC Connections to Ama		PASSED FAILED FAILED PASSED PASSED PASSED PASSED FAILED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED	
IAA25 MEA should be enabled for all IAM users that have a console password           IAA26 Hardware MEA should be enabled for the root user           IAA27 Password policies for IAM users should have strong configurations           IAA8 Unused IAM user credentials should have strong configurations on all KMS keys           KMS:1 IAM customer managed policies should not allow decryption actions on all KMS keys           KMS:2 IAM principals should not have IAM infine policies that allow decryption actions on all KMS keys           KMS:3 AWS KMS keys should not be delated unintentionally           Lambda1 Lambda functions should use supported runtimes           Lambda.4 Lambda functions should be ada-letter queue configured           RDS:11 RDS anapohot should be private           RDS:11 RDS anapohot should be configured for RDS instances           RDS:12 IAM authentication should be configured for RDS clusters           RDS:13 RDS automatic minor version upgrades should be enabled           RDS:14 Amazon Aurora clusters should have backtracking enabled           RDS:24 RDS DB instances should have encryption at-rest enabled           RDS:55 RDS DB instances should have deletion protection enabled           RDS:57 RDS all instances should have deletion protection enabled           RDS:57 RDS DB instances should have deletion protection enabled           RDS:57 RDS DB instances should have deletion protection enabled           RDS:57 RDS Clusters should have deletion protection enabled <t< td=""><td></td><td>PASSED FAILED FAILED PASSED PASSED PASSED PASSED FAILED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED</td><td></td></t<>		PASSED FAILED FAILED PASSED PASSED PASSED PASSED FAILED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED	
IAM.5 MFA should be enabled for all IAM users that have a console password           IAM.6 Hardware MFA should be enabled for the root user           IAM.7 Password policies for IAM users should have strong configurations           IAM.8 Unused IAM user credentials should be removed           KMS.1 IAM customer managed policies should not allow decryption actions on all KMS keys           KMS.2 IAM principals should not have IAM infline policies that allow decryption actions on all KMS keys           KMS.2 IAM principals should not be deleted unintentionally           Lambda 1 Lambda function policies should prohibit public access           Lambda 2. Lambda function should as supported runtimes           Lambda 4. Lambda function should have adead-letter queue configured           RDS.10 IAM authentication should be configured for RDS instances           RDS.11 AM authentication should be configured for RDS clusters           RDS.12 IAM authentication should have backtracking enabled           RDS.13 RDS automatic minor version upgrades should be enrypted at rest           RDS.24 RDS DB Instances should have canfigured for RDS DB Instances           RDS.24 RDS DB Instances should have canfigured for RDS lastances           RDS.24 RDS DB Instances should have canfigured for RDS DB Instances           RDS.24 RDS DB Instances should have canfigured for RDS DB Instances           RDS.24 RDS DB Instances should have canfigured for RDS DB Instances           RDS.44 RDS cluster snapehots and database supphots s		PASSED FAILED FAILED PASSED PASSED PASSED PASSED FAILED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED PASSED	
IAM.5 MFA should be enabled for III IAM users that have a console password           IAM.6 Hardware MFA should be enabled for the root user           IAM.7 Password policies for IAM users should have strong configurations           IAM.8 Unused IAM user credentials should be removed           KMS.1 IAM customer managed policies should net allow decryption actions on all KMS keys           KMS.2 IAM principals should not have IAM inline policies that allow decryption actions on all KMS keys           KMS.3 AWS KMS keys should not be deleted unintentionally           Lambda 1. Lambda function policies should prohibit public access           Lambda 2. Lambda functions should be and i-tere queue configured           RDS.10 IAM authentication should be configured for RDS instances           RDS 103 RM submit cation should have a decat-ieter queue configured           RDS 103 RM authentication should have backtracking enabled           RDS 103 RM authentication should have backtracking enabled           RDS 103 RDS automatic minor version upgrades should be enabled           RDS 2.8 DS DB Instances should have backtracking enabled           RDS 2.8 DS DB Instances should have encryption at-rest enabled           RDS 4.8 DS DB Instances should be configured for RDS DB Instances           RDS 4.8 DS DB Instances should have encryption at-rest enabled           RDS 4.8 DS DB Instances should have encryption at-rest enabled           RDS 4.8 DS DB Instances should be configured for RDS DB Instances		PASSEDFAILEDFAILEDPASSED	
IAAS SMFA should be enabled for III IAAI users that have a console password           IAAS Flandware MFA should be enabled for the root user           IAAS Password policies for IAM users should have strong configurations           IAAS Unused IAM user credentials should be removed           KMS.1 IAM customer managed policies should not allow decryption actions on all KMS keys           KMS.2 IAM principals should not have IAM infine policies that allow decryption actions on all KMS keys           KMS.3 AWS KMS keys should not have IAM infine policies that allow decryption actions on all KMS keys           Lambda 1 Lambda functions should use supported runtimes           Lambda 2 Lambda functions should be configured for RDS instances           RDS.10 IAM authentication should be configured for RDS clusters           RDS.11 KM authentication should have backtracking enabled           RDS.2 RDS DB Instances should parbible public access, determined by the PubliclyAccessible configuration           RDS.3 RDS DB instances should be configured for RDS DB instances           RDS.4 RDS cluster sapshots and database sapshots should be encrypted at rest           RDS.4 RDS DB instances should be configured with multiple Availability Zones           RDS.4 RDS DB instances should be configured with multiple Availability Zones           RDS.4 RDS Clusters should have deletion protection enabled           RDS.4 RDS DB instances should be configured tor RDS DB instances           RDS.4 RDS DB instances should be configured tor RDS DB instanc		PASSEDFAILEDFAILEDPASSED	
IAAS bills should be enabled for all IAA users that have a console password           IAAS bilandware MiKA should be enabled for the root user           IAAS Password policies for IAM users should have strong configurations           IAAS Unused IAM user credentials should be removed           KMS-11MA customer managed policies should not allow decryption actions on all KMS keys           KMS-21AM principals should not have IAM infine policies that allow decryption actions on all KMS keys           KMS-21AM principals should not be deleted unintontionally           Lambda 1 Lambda functions should use supported runtimes           Lambda 1 Lambda functions should be configured for RDS instances           RDS-11AD songehot should be configured for RDS clusters           RDS-11AD automatic minor version upgrades should he enabled           RDS-11AD automatic minor version upgrades should be encrypted at rest           RDS-11AD clusters should have backtracking enabled           RDS-11SD DB instances should have encryption at-rest enabled           RDS-11AD clusters mayshots and database sangshots should be encrypted at rest           RDS-11SD DB instances should have deletion protection enabled           RDS-12 KMB clusters mayshots have deletion protection enabled           RDS-13 RDS DB instances should have automatic sangshots should be encrypted at rest           RDS-13 RDS DB instances should have automatic sangshots enabled           RDS-14 Amazon Redshift clusters should prohibit public access.		PASSEDFAILEDFAILEDPASSED	
IAAS MFA should be enabled for all IAM users that have a console passoord           IAAG Hardware MFA should be enabled for the root user           IAA7 Password policies for IAM users should have strong configurations           IAAS Unused IAM user credentials should be removed           IAAS 2 MAR customer managed policies should not allow decryption actions on all KMS keys           IAMS 2 MA principals should not have IAM inline policies that allow decryption actions on all KMS keys           IAMS 2 MA principals should not be deleted unintentionally           IAmbda 1 Lambda function should use supported runtimes           IAmbda 2 Lambda functions should use supported runtimes           IAMS 2 MA autonition should be configured for RDS instances           RDS 10 MA authentication should be configured for RDS instances           RDS 114 Martentication should be configured for RDS olusters           RDS 114 Martentication should be configured for RDS olusters           RDS 115 RDS automatic minor version upgrades should be encrypted at rest           RDS 2 RDS DB Instances should have activating enabled           RDS 3 RDS DB Instances should have activating enabled           RDS 4 RDS cluster snapshots should be configured for RDS DB instances           RDS 4 RDS Cluster snapshots and database anapshots should be encrypted at rest           RDS 4 RDS Cluster snapshots and database anapshots should be encrypted at rest           RDS 4 RDS Cluster should have deletion protection enabled		PASSEDFAILEDFAILEDPASSED	
IAAS MFA should be enabled for all IAM users that have a console passeord           IAM 6 Hardware MFA should be enabled for the root user           IAAS 7 Passeord policies for IAM users should have strong configurations           IAAS Unused IAM user credentials should be removed           IAAS 2 MAR customer managed policies should not allow decryption actions on all KMS keys           IAAS 3 AWS KMS keys should not have IAM inline policies that allow decryption actions on all KMS keys           IAAS 2 MAP principals should not have IAM inline policies that allow decryption actions on all KMS keys           IAM54.2 Lambda function policies should not halve was credentianally           Lambda 1 Lambda function should be deleted unintentionally           IAM54.3 AWS KMS keys should not be deleted unintentionally           IAM54.4 Lambda function should be configured for RDS instances           ROS1 RDS snapshot should use supported runtimes           IAM54.4 Lambda functions should have a dead-letter queue configured           ROS1 RDS snapshot should be configured for RDS blatters           ROS1 RDS snapshot should be configured for RDS blatters           ROS1 RDS DB Instances should have activating enabled           ROS2 RDS DB Instances should have activating enabled           ROS2 RDS DB Instances should have activation enabled           ROS2 RDS DB Instances should have deletion protection enabled           ROS2 RDS DB Instances should have deletion protection enabled		PASSEDFAILEDFAILEDPASSED	
IAU.S. MFA should be enabled for ill IAM users that have a console passoord           IAM.S. Hardware MFA should be enabled for the root user           IAM.Z. Password policies for IAM users should have strong configurations           IAM.S. Unused IAM user credentials should be removed           IAM.S. TAM cuistomer managed policies should not allow decryption actions on all KMS keys           IAM.S. AWS KMS keys should not ba deleted unitertionally           Lambda.1. Lambda functions should prohibili polici access           Lambda.2. Lambda functions should prohibili polici access           RDS.1.RDS anapohet should be errored           RDS.1.RDS anapohet should be configured for RDS instances           RDS.1.RDS anapohet should be configured for RDS clusters           RDS.1.RDS anapohet should be configured for RDS clusters           RDS.1.RDS anapohet should be configured for RDS clusters           RDS.1.RDS automatic minor version upgrades should be enabled           RDS.2.RDS DB Instances should have access, determined by the PubliclyAccessible configuration           RDS.3.RDS DB instances should have access, determined by the PubliclyAccessible configuration           RDS.3.RDS DB instances and ubbase enceptote on mabled           RDS.4.RDS alusters anapohors and database enceptote on anabled           RDS.4.RDS DB instances should have acternative parables           RDS.4.RDS alusters anapohors and database enceptotes thauit be encrysted in tremsit           RDS.4.RDS		PASSEDFAILEDFAILEDPASSED	
IAAS MFA should be enabled for ithe root user           IAAS Paraware MFA should be enabled for the root user           IAAS Password policies for IAM users should have strang configurations           IAAS Database policies for IAM users should have strang configurations           IAAS Unused IAM user credentials should be removed           KMS-11MA customer managed policies should not allow decryption actions on all KMS keys           IAMS ANS MAS keys should not be deleted unintentionally           Lambda Lambda function should not be deleted unintentionally           IAMS Should be enabled for the enapported runtimes           IAMS Should a function should use algoprited runtimes           RDS 10 MA authentication should be configured for RDS instances           RDS 11 MS shaphet should have a cead-letter queue configured           RDS 11 MS anomatic minor version upgrades should to enabled           RDS 12 MA authentication should be configured for RDS clusters           RDS 20 SD Bit strances should have acceryption at-rest enabled           RDS 20 SD Bit strances should have deletion protection enabled           RDS 20 RDS DB itstances should have deletion protection enabled           RDS 20 RDS DB itstances should have deletion protection enabled           RDS 20 RDS BD Bitstances should have deletion protection enabled           RDS 20 RDS DB itstances should have deletion protection enabled           RDS 20 RDS 20 Rot stances should have deletion protection enabled		PASSEDFAILEDFAILEDPASSED	
IAM 6 Mirk a should be enabled for all IAM users that have a console password           IAM 6 Hurdware MFA should be enabled for the root user           IAM 7 Password policies for IAM users should here strong configurations           IAM 8 Junced IAM user credentials should be removed           IAM 5 AWS XMS keys should not be delated unintentionally           IAM 5 AWS XMS keys should not be delated unintentionally           IAM 5 Junk 4 Junced IAM users should be robited attraited decryption actions on all KMS keys           IAM 5 AWS XMS keys should not be delated unintentionally           IAM 5 Junk 4 Junk 6 Intertions should use supported runtimes           IAM 5 Junk 4 Junk 6 Intertions should use supported runtimes           IAM 5 JUNK 4 Junk 6 Intertions should use supported runtimes           IAM 5 JUNK 4 Junk 6 Intertions should here onligered for RDS Instances           IAM 5 JUNK 4 Junk 6 Intertions should here onligered for RDS Instances           IAM 5 JUNK 4 JUNK 4 JUNK 6 INFORE Should be enabled           IADS 14 Ma authentication should here onligered for RDS Instances           IADS 14 RAM 6 Instances should here onligered for RDS Instances           IADS 14 RAM 6 Instances should here onligered for RDS Instances           IADS 14 RAM 6 Instances should here onligered for RDS Instances           IADS 14 RAM 6 Instances should here onligered for RDS Instances           IADS 14 RDS DB Instances should here onligered for RDS Instances           IADS 14 RDS Instan		PASSEDFAILEDFAILEDPASSED	
IAM 5 MFA should be enabled for hit root user           IAMA 5 MFA should be enabled for the root user           IAMA 7 Passeword palieles for MA users should have strang configurations           IAMA 10 user concentrates should be removed           IAMA 5 MFA data user concentrates should not allow decryption actions on all KMS keys           IAMA 5 MA work Concentrates should not have AM inline policies that allow decryption actions on all KMS keys           IAMA 5 MAS KMS keys should not have AM inline policies that allow decryption actions on all KMS keys           IAMA 5 MAS KMS keys should not have AM inline policies that allow decryption actions on all KMS keys           IAMA 5 MAS KMS keys should not have AM inline policie access           Iamabda 1 Lambda functions should use supported runtimes           Iamabda 2 Lambda functions should have a decel-letter queue configured           RDS 14 Ma submitication should be configured for RDS clusters           RDS 14 Ma submitication should have takeKhracking enabled           RDS 14 Ma submitication should have takeKhracking enabled           RDS 2 RDS DB Instances should probabili quable access, dotormined by the PubliclyAccessible configuration           RDS 3 RDS 2 BD DB Instances should have deletion protection enabled           RDS 14 Marazin Autoria dubbe configured for RDS DB Instances           RDS 2 RDS DB Instances should have deletion protection enabled           RDS 14 S Batabase lagging should be configured for RDS DB Instances <td< td=""><td></td><td>PASSEDFAILEDFAILEDPASSED</td><td></td></td<>		PASSEDFAILEDFAILEDPASSED	
IAAS SAFA should be enabled for all IAM users that have a console password           IAAG Hardware AFA should be enabled for the root user           IAAG Password policies for IAM users should have a strong configurations           IAAS JIAAM customer managed policies should nor allow decryotion actions on all KMS keys           IAAS SANS KAS keys should not bave IAM initiantionally           IAAM SANS KAS keys should not be deleted unitiantionally           IAAMS ALL ambde functions should use supported unitimes           IAAMS ALL ambde functions should use supported runtimes           IAAMS ALL ambde functions should use configured for IADS elusters           IAAMS ALL ambde functions should use configured for IADS elusters           IAAMS DE Submather should be configured for IADS elusters           IAMS DE Submather should have access, determined by the Public/vaccessible configuration           IAMS DE Submather should have access, determined by the Public/vaccessible configuration           IAMS DE Submather should have actionged for IADS DE Instances           IAMS DE Submather should have actionged for IADS DE Instances           IAMS DE Submathe		PASSEDFAILEDFAILEDPASSED	
IAAS NKA should be embled for all IAM users that have a cancele passward           IAAB Hardware NKA should be embled for the root user           IAAB Unued IAM user or edentials should be removed           IAAB Cancel To the root user           IAAB Shardware NKA should not be emboded           IAAB Cancel To the removed           IAAB Shardware the IAM user or edentials should be removed           IAAB SA WKS KMS keys should not be eletted unimentionally           Lambda Lambda functions obtaid and be eletted unimentionally           Lambda Lambda functions should not be eletted unimentionally           Lambda Lambda functions obtaid and the configured for fIDS instances           RDS 10 IAM authentication should be exceeded removed           RDS 10 IAM authentication should be configured for fIDS instances           RDS 11 AM authentication should be configured for fIDS instances           RDS 12 IAM authentication should be configured for fIDS instances           RDS 13 RDS auternatic minar version upgrades should her maryptical at rest           RDS 14 Anazan Aurara clusters should have backfracking erabled           RDS 15 RDS DB instances should and enabled           RDS 16 RDS DB Instances should have deletion protection enabled           RDS 7 RDS PID instances should have deletion protection enabled           RDS 7 RDS DB Restances should have deletion protection enabled           RDS 7 RDS Rol statuces should have automatic ungrades to major		PASSEDFAILEDFAILEDPASSED	
IAAS NEG activate M A should be enabled for the root user           IAAS Factivate M A should be enabled for the root user           IAAS Factivate M A should be enabled for the root user           IAAS Taxes and the enabled for the root user           IAAS Taxes and the enabled for the root user           IAAS Taxes and the enabled for the root user           IAAS Taxes and the enabled for the objects should be enabled           IAAS Taxes and the enabled for the objects should be enabled           IAAS Taxes and the objects should prohibit public access           IAAM authentication should like supported runtimes           IAMS TAXEs and the object of the root user of the object of the root users           IABS TAXEs and the object of the root users           IABS TAXEs and the object of the root users           IABS TAXEs and the object of the root users           IABS TAXEs and the object of the root users           IABS TAXEs and the object of the root users           IABS TAXEs and the object of the root users           IABS TAXEs and the object of the root users           IABS TAXEs and the object of the root users           IABS TAXEs and the object of the root users           IABS TAXEs and the object of the root users           IABS TAXEs and the object of the root users           IABS TAXES and the object of the root users           IABS TAXES and the object of the root users		PASSEDFAILEDFAILEDPASSED	

# CIS AWS Foundations Benchmark v1.2.0

The CIS AWS Foundations Benchmark describes a set of security guidelines that have been developed by the cyber security community. These best practices and recommendations are intended to be used by anyone who uses the AWS platform. This standard presents specific recommendations on a variety of essential operations in any cloud platform environment, including access management, monitoring, logging, storage, and network configuration.











Controls

The table below presents a summary of the status of each control in this security standard and its status for each region in which it was evaluated. Some controls are evaluated multiple times for multiple assets

Control	us-east-1	us-east-2	us-west-2
1.1 Avoid the use of the "root" account	FAILED	FAILED	FAILED
1.10 Ensure IAM password policy prevents password reuse		FAILED	
1.11 Ensure IAM password policy expires passwords within 90 days or less		FAILED	
1.12 Ensure no root account access key exists		PASSED	
1.13 Ensure MFA is enabled for the "root" account		FAILED	
1.14 Ensure hardware MFA is enabled for the "root" account		FAILED	
1.16 Ensure IAM policies are attached only to groups or roles		PASSED	
1.2 Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password		PASSED	
1.20 Ensure a support role has been created to manage incidents with AWS Support		FAILED	
1.22 Ensure IAM policies that allow full "*:*" administrative privileges are not created		PASSED	
1.3 Ensure credentials unused for 90 days or greater are disabled		PASSED	
1.4 Ensure access keys are rotated every 90 days or less		PASSED	
1.5 Ensure IAM password policy requires at least one uppercase letter		FAILED	
1.6 Ensure IAM password policy requires at least one lowercase letter		FAILED	
1.7 Ensure IAM password policy requires at least one symbol		FAILED	
1.8 Ensure IAM password policy requires at least one number		FAILED	
1.9 Ensure IAM password policy requires minimum password length of 14 or greater		FAILED	
2.2 Ensure CloudTrail log file validation is enabled		PASSED	
2.4 Ensure CloudTrail trails are integrated with CloudWatch Logs		PASSED	
2.5 Ensure AWS Config is enabled	FAILED	FAILED	FAILED
2.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs		PASSED	
2.8 Ensure rotation for customer created CMKs is enabled		PASSED	
2.9 Ensure VPC flow logging is enabled in all VPCs		FAILED	
3.1 Ensure a log metric filter and alarm exist for unauthorized API calls	FAILED	FAILED	FAILED
3.10 Ensure a log metric filter and alarm exist for security group changes	FAILED	FAILED	FAILED
3.11 Ensure a log metric filter and alarm exist for changes to Network Access Control Lists (NACL)	FAILED	FAILED	FAILED
3.12 Ensure a log metric filter and alarm exist for changes to network gateways	FAILED	FAILED	FAILED
3.13 Ensure a log metric filter and alarm exist for route table changes	FAILED	FAILED	FAILED
3.14 Ensure a log metric filter and alarm exist for VPC changes	FAILED	FAILED	FAILED
3.2 Ensure a log metric filter and alarm exist for Management Console sign-in without MFA	FAILED	FAILED	FAILED
3.3 Ensure a log metric filter and alarm exist for usage of "root" account	FAILED	FAILED	FAILED
3.4 Ensure a log metric filter and alarm exist for IAM policy changes	FAILED	FAILED	FAILED
3.5 Ensure a log metric filter and alarm exist for CloudTrail configuration changes	FAILED	FAILED	FAILED
3.6 Ensure a log metric filter and alarm exist for AWS Management Console authentication failures	FAILED	FAILED	FAILED
3.7 Ensure a log metric filter and alarm exist for disabling or scheduled deletion of customer created CMKs	FAILED	FAILED	FAILED
3.8 Ensure a log metric filter and alarm exist for S3 bucket policy changes	FAILED	FAILED	FAILED
3.9 Ensure a log metric filter and alarm exist for AWS Config configuration changes	FAILED	FAILED	FAILED
4.1 Ensure no security groups allow ingress from 0.0.0.0/0 to port 22		PASSED	
4.2 Ensure no security groups allow ingress from 0.0.0.0/0 to port 3389		PASSED	
4.3 Ensure the default security group of every VPC restricts all traffic		FAILED	

# PCI DSS v3.2.1

The Payment Card Industry Data Security Standard (PCI DSS) documents a mapping of PCI DSS requirements into an AWS architecture. This AWS Security Hub implemention of a subset of the PCI requirements helps users utilize automated testing of compliance with these requirements. Though these controls have been developed for systems that handle cardholder data, they represent a set of best practices that could be beneficial to all cloud platform users.

Findings by severity The chart below shows the high level severity of the findings for this security standard

Findings status by region The chart below shows the status of the findings for this security standard by AWS region







Evaluated asset classes by region

The chart below shows the number of findings for different categories of AWS assets for each region



Controls

The table below presents a summary of the status of each control in this security standard and its status for each region in which it was evaluated. Some controls are evaluated multiple times for multiple assets

Control	us-east-1	us-east-2
PCI.AutoScaling.1 Auto scaling groups associated with a load balancer should use load balancer health checks		PASSED
PCI.CW.1 A log metric filter and alarm should exist for usage of the "root" user	FAILED	FAILED
PCI.CloudTrail.1 CloudTrail logs should be encrypted at rest using AWS KMS CMKs		PASSED
PCI.CloudTrail.2 CloudTrail should be enabled		FAILED
PCI.CloudTrail.3 CloudTrail log file validation should be enabled		PASSED
PCI.CloudTrail.4 CloudTrail trails should be integrated with Amazon CloudWatch Logs		PASSED
PCI.CodeBuild.1 CodeBuild GitHub or Bitbucket source repository URLs should use OAuth		PASSED
PCI.CodeBuild.2 CodeBuild project environment variables should not contain clear text credentials		PASSED
PCI.Config.1 AWS Config should be enabled	FAILED	FAILED
PCI.DMS.1 Database Migration Service replication instances should not be public		PASSED
PCI.EC2.1 EBS snapshots should not be publicly restorable		PASSED
PCI.EC2.2 VPC default security group should prohibit inbound and outbound traffic		FAILED
PCI.EC2.3 Unused EC2 security groups should be removed		FAILED
PCI.EC2.4 Unused EC2 EIPs should be removed		PASSED
PCI.EC2.5 Security groups should not allow ingress from 0.0.0.0/0 to port 22		PASSED
PCI.EC2.6 VPC flow logging should be enabled in all VPCs		FAILED
PCI.ELBv2.1 Application Load Balancer should be configured to redirect all HTTP requests to HTTPS		PASSED
PCI.ES.1 Amazon Elasticsearch Service domains should be in a VPC		PASSED
PCI.ES.2 Elasticsearch domains should have encryption at-rest enabled		PASSED
PCI.GuardDuty.1 GuardDuty should be enabled		FAILED
PCI.IAM.1 IAM root user access key should not exist		PASSED
PCI.IAM.2 IAM users should not have IAM policies attached		PASSED
PCI.IAM.3 IAM policies should not allow full "*" administrative privileges		PASSED
PCI.IAM.4 Hardware MFA should be enabled for the root user		FAILED
PCI.IAM.5 Virtual MFA should be enabled for the root user		FAILED
PCI.IAM.6 MFA should be enabled for all IAM users		PASSED
PCI.IAM.7 IAM user credentials should be disabled if not used within a pre-defined number days		PASSED
PCI.IAM.8 Password policies for IAM users should have strong configurations		FAILED
PCI.KMS.1 Customer master key (CMK) rotation should be enabled		PASSED
PCI.Lambda.1 Lambda functions should prohibit public access		PASSED
PCI.Lambda.2 Lambda functions should be in a VPC		FAILED
PCI.RDS.1 RDS snapshot should be private		PASSED
PCI.RDS.2 RDS DB Instances should prohibit public access		PASSED
PCI.Redshift.1 Amazon Redshift clusters should prohibit public access		PASSED
PCI.S3.1 S3 buckets should prohibit public write access		PASSED
PCI.S3.2 S3 buckets should prohibit public read access		PASSED
PCI.S3.3 S3 buckets should have cross-region replication enabled		FAILED
PCI.S3.4 S3 buckets should have server-side encryption enabled		FAILED
PCI.S3.5 S3 buckets should require requests to use Secure Socket Layer		FAILED
PCI.S3.6 S3 Block Public Access setting should be enabled		FAILED
PCI.SSM.1 EC2 instances managed by Systems Manager should have a patch compliance status of COMPLIANT after a patch installation		PASSED
PCI.SSM.2 EC2 instances managed by Systems Manager should have an association compliance status of COMPLIANT		PASSED
PCI.SSM.3 EC2 instances should be managed by AWS Systems Manager		FAILED
PCI.SageMaker.1 Amazon SageMaker notebook instances should not have direct internet access		PASSED