SignetRisk
CLOUD COMPLIANCE

AWS Azure GCP

Testfirstname Testlastname

Amazon Web Services Cyber Risk Report

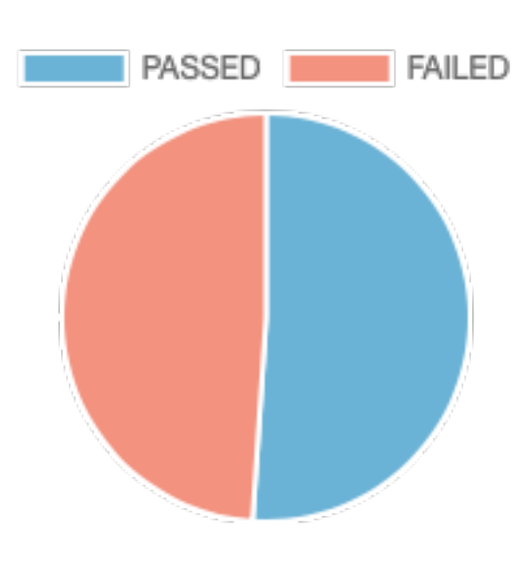
AWS Cyber Risk Summary

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	

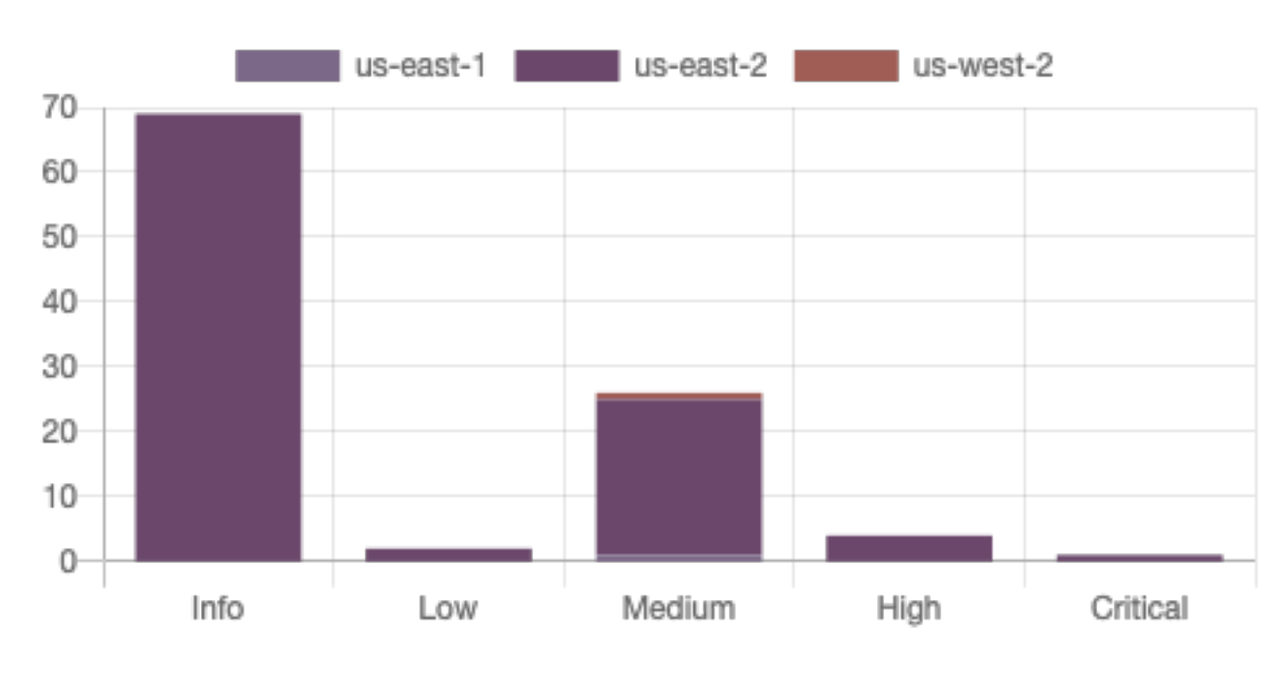
Total number of passed versus failed controls
The chart below represents the relative number of tests that passed versus tests that failed across all standards, regardless of their importance or criticality.



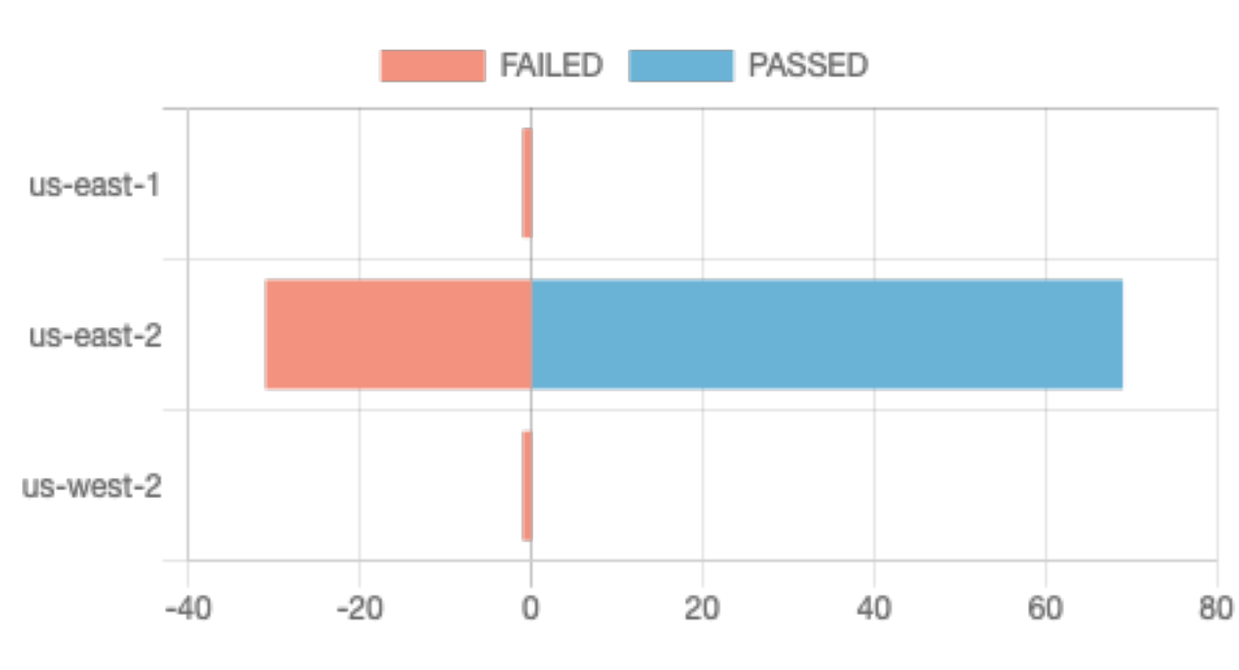
AWS Foundational Security Best Practices v1.0.0

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.

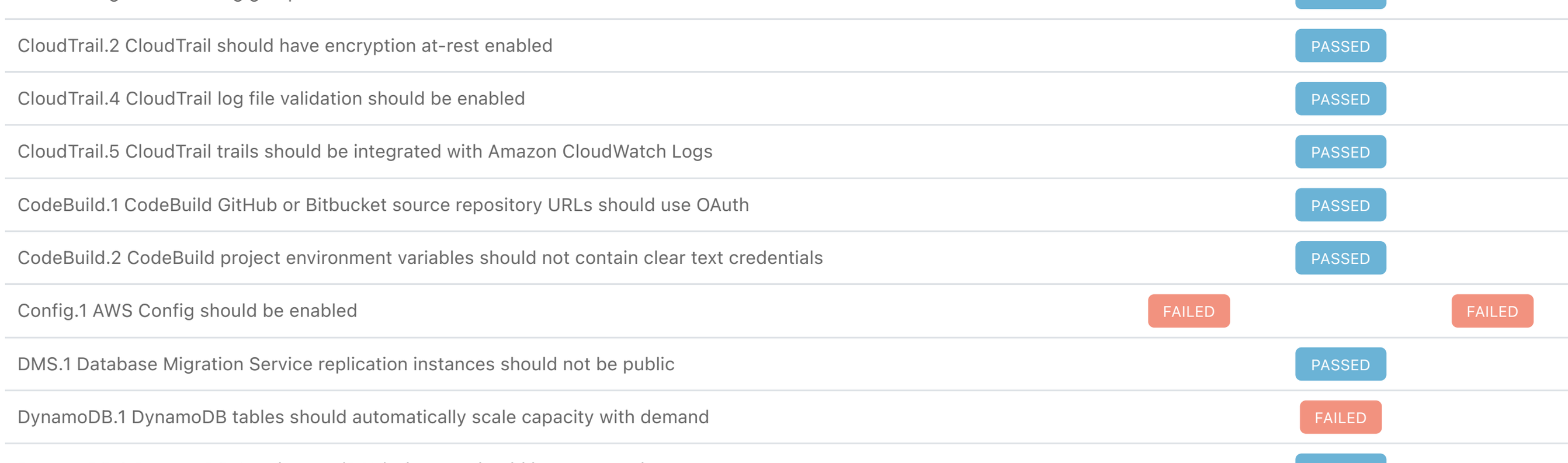
Findings by severity
The chart below shows the high level severity of the findings for this security standard



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



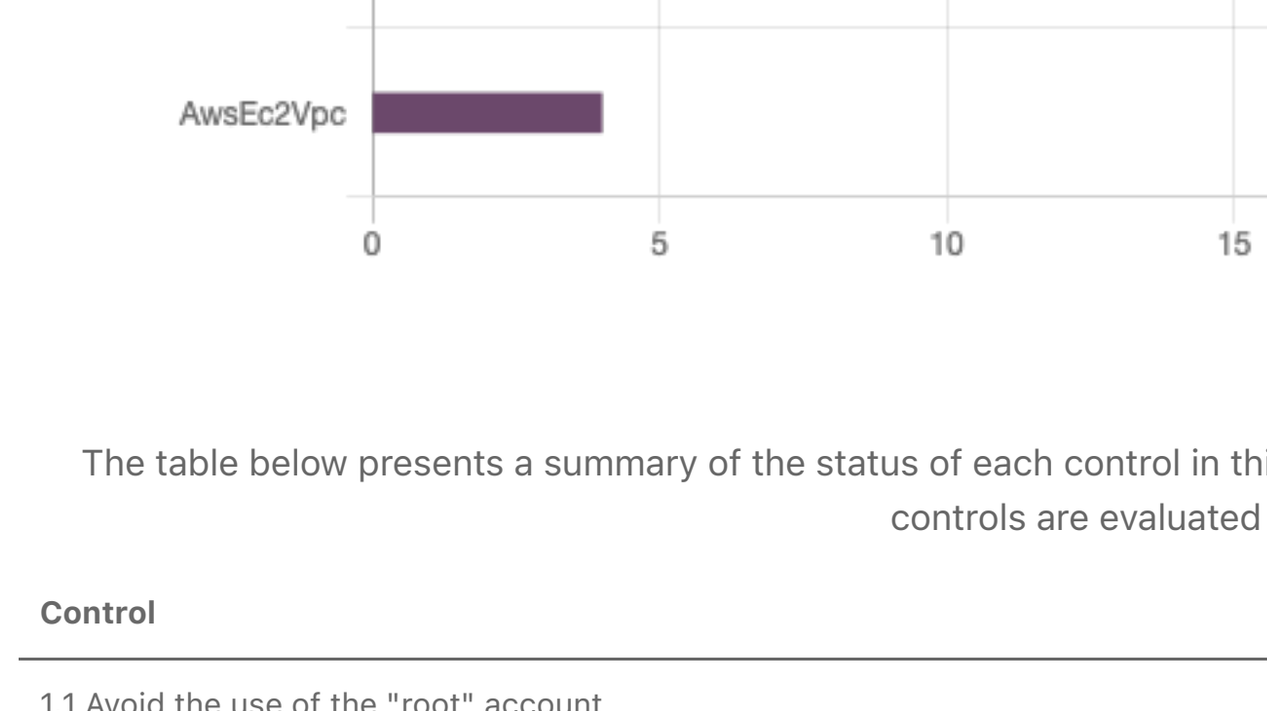
Controls
The table below presents a summary of the status of each control in this security standard and its status for each region in which it was evaluated. Some controls are evaluated multiple times for multiple assets

Control	us-east-1	us-east-2	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	
CodeBuild.1 CodeBuild GitHub or Bitbucket source repository URLs should use OAuth		PASSED	
CodeBuild.2 CodeBuild project environment variables should not contain clear text credentials		PASSED	
Config.1 AWS Config should be enabled	FAILED		FAILED
DMS.1 Database Migration Service replication instances should not be public		PASSED	
DynamoDB.1 DynamoDB tables should automatically scale capacity with demand		FAILED	
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 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	
EFS.2 Amazon EFS volumes should be in backup plans		PASSED	
ELB.3 Classic Load Balancer listeners should be configured with HTTPS or TLS termination		PASSED	
ELB.4 Application load balancer should be configured to drop http headers		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 MFA should be enabled for all IAM users that have a console password		PASSED	
IAM.6 Hardware MFA should be enabled for the root user		FAILED	
IAM.7 Password policies for IAM users should have strong configurations		FAILED	
IAM.8 Unused IAM user credentials should be removed		PASSED	
KMS.1 IAM customer managed policies should not allow decryption actions on all KMS keys		PASSED	
KMS.2 IAM principals should not have IAM inline policies that allow decryption actions on all KMS keys		PASSED	
KMS.3 AWS KMS keys should not be deleted unintentionally		PASSED	
Lambda.1 Lambda function policies should prohibit public access		PASSED	
Lambda.2 Lambda functions should use supported runtimes		PASSED	
Lambda.4 Lambda functions should have a dead-letter queue configured		FAILED	
RDS.1 RDS snapshot should be private		PASSED	
RDS.10 IAM authentication should be configured for RDS instances		PASSED	
RDS.12 IAM authentication should be configured for RDS clusters		PASSED	
RDS.13 RDS automatic minor version upgrades should be enabled		PASSED	
RDS.14 Amazon Aurora clusters should have backtracking enabled		PASSED	
RDS.2 RDS DB Instances should prohibit public access, determined by the PubliclyAccessible configuration		PASSED	
RDS.3 RDS DB instances should have encryption at-rest enabled		PASSED	
RDS.4 RDS cluster snapshots and database snapshots should be encrypted at rest		PASSED	
RDS.5 RDS DB instances should be configured with multiple Availability Zones		PASSED	
RDS.6 Enhanced monitoring should be configured for RDS DB instances		PASSED	
RDS.7 RDS clusters should have deletion protection enabled		PASSED	
RDS.8 RDS DB instances should have deletion protection enabled		PASSED	
RDS.9 Database logging should be enabled		PASSED	
Redshift.1 Amazon Redshift clusters should prohibit public access		PASSED	
Redshift.2 Connections to Amazon Redshift clusters should be encrypted in transit		PASSED	
Redshift.3 Amazon Redshift clusters should have automatic snapshots enabled		PASSED	
Redshift.6 Amazon Redshift should have automatic upgrades to major versions enabled		PASSED	
Redshift.7 Redshift clusters should use enhanced VPC routing		PASSED	
S3.1 S3 Block Public Access setting should be enabled		FAILED	
S3.2 S3 buckets should prohibit public read access		PASSED	
S3.3 S3 buckets should prohibit public write access		PASSED	
SSM.2 EC2 instances managed by Systems Manager should have a patch compliance status of COMPLIANT after a patch installation		PASSED	
SSM.3 EC2 instances managed by Systems Manager should have an association compliance status of COMPLIANT		PASSED	
SageMaker.1 Amazon SageMaker notebook instances should not have direct internet access		PASSED	
SecretsManager.1 Secrets Manager secrets should have automatic rotation enabled		PASSED	
SecretsManager.2 Secrets Manager secrets configured with automatic rotation should rotate successfully		PASSED	
SecretsManager.3 Remove unused Secrets Manager secrets		PASSED	
SecretsManager.4 Secrets Manager secrets should be rotated within a specified number of days		PASSED	

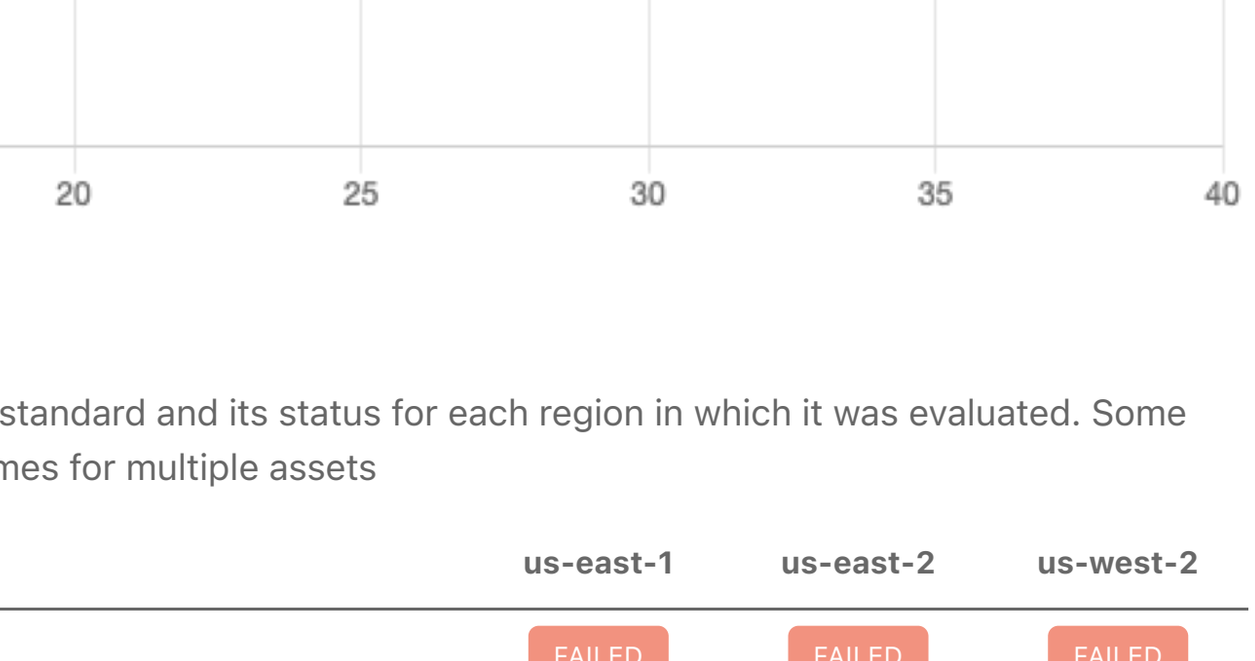
CIS AWS Foundations Benchmark v1.2.0

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.

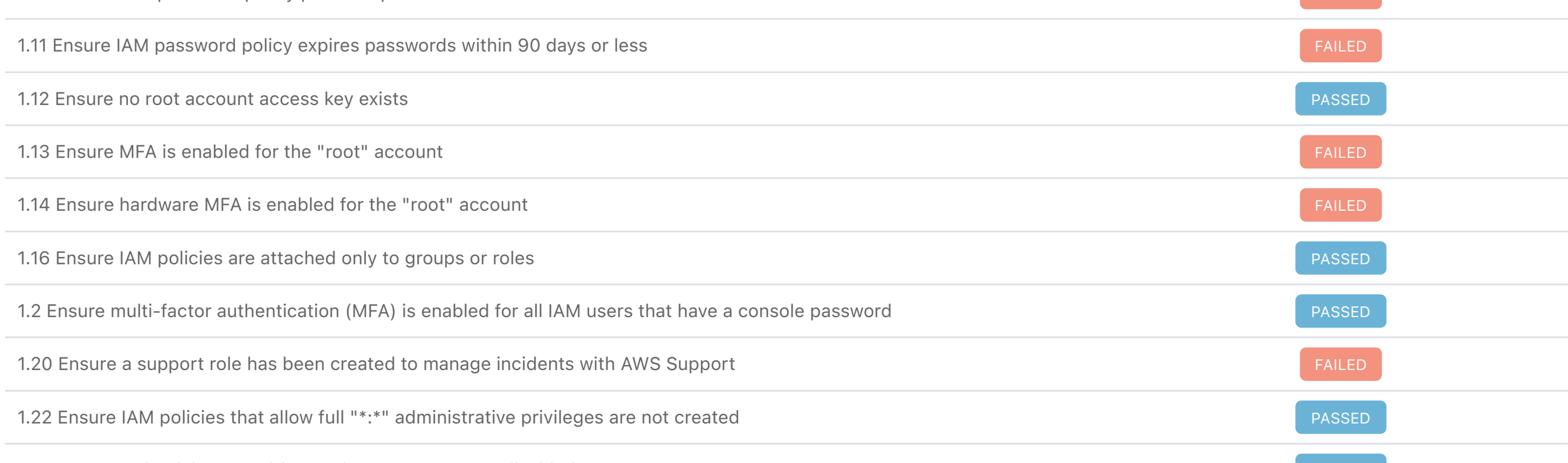
Findings by severity
The chart below shows the high level severity of the findings for this security standard



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



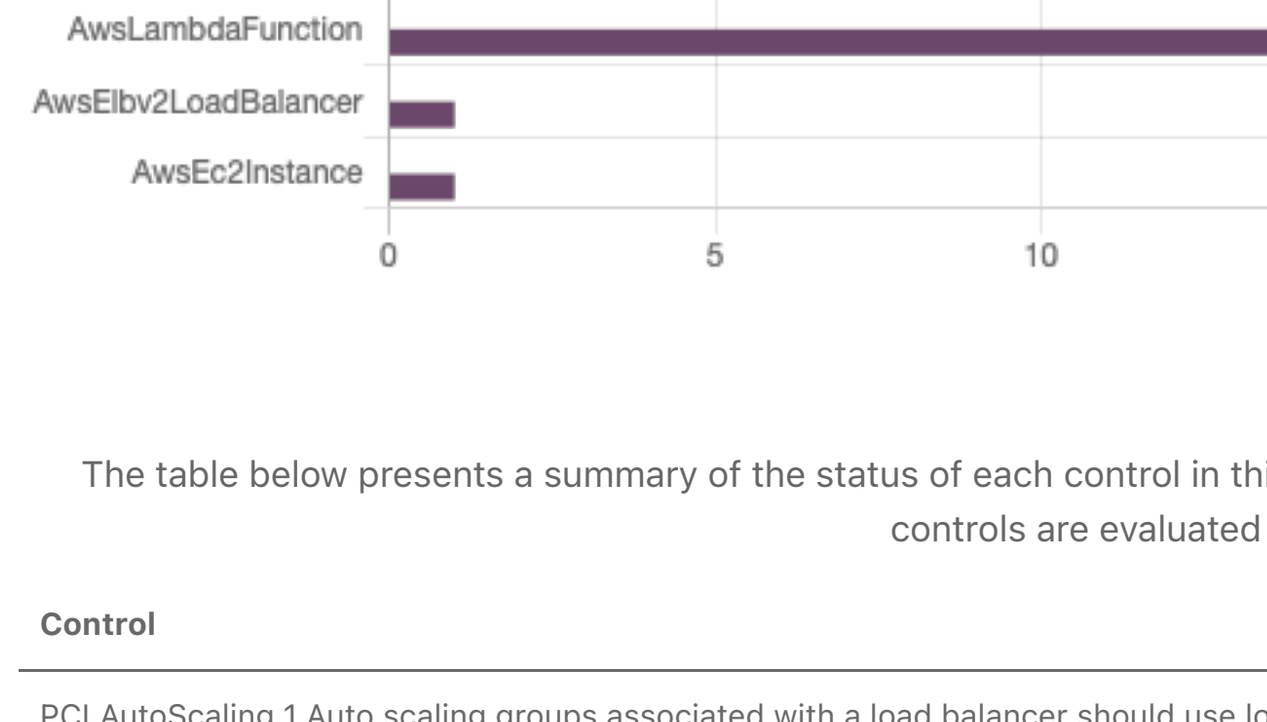
Controls
The table below presents a summary of the status of each control in this security standard and its status for each region in which it was evaluated. Some controls are evaluated multiple times for multiple assets

Control	us-east-1	us-east-2	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	

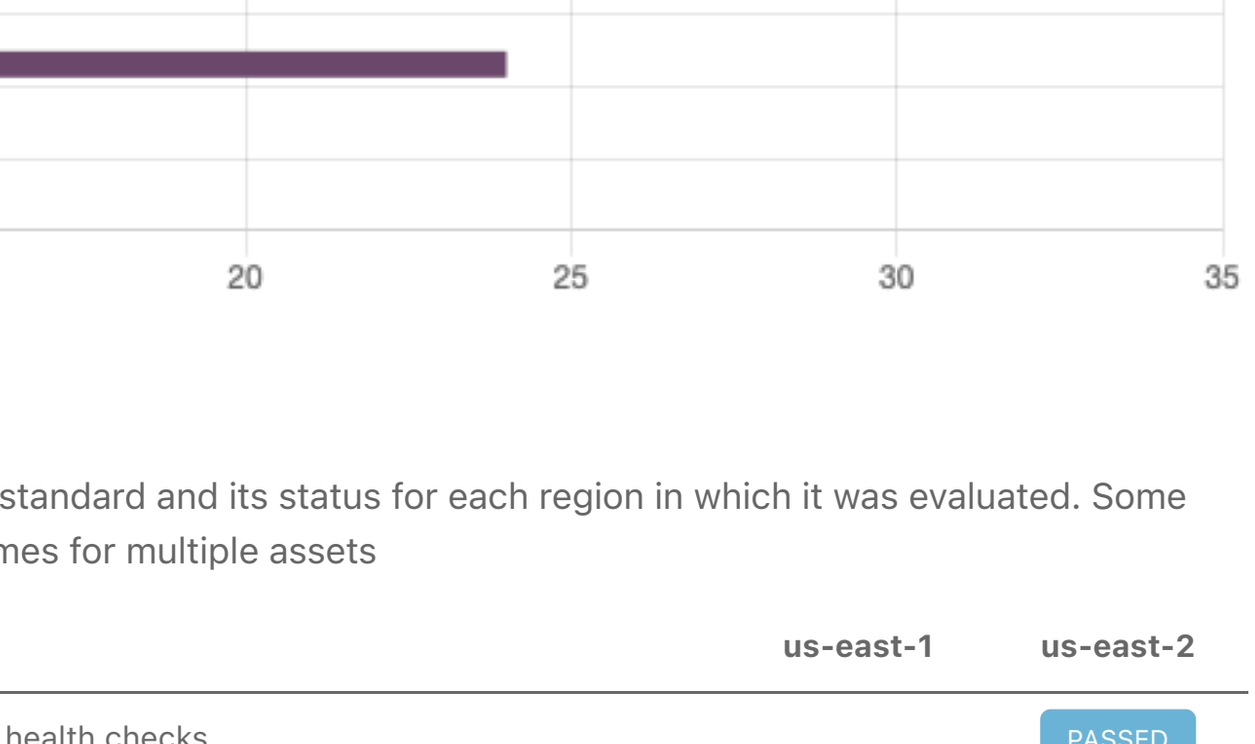
PCI DSS v3.2.1

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.

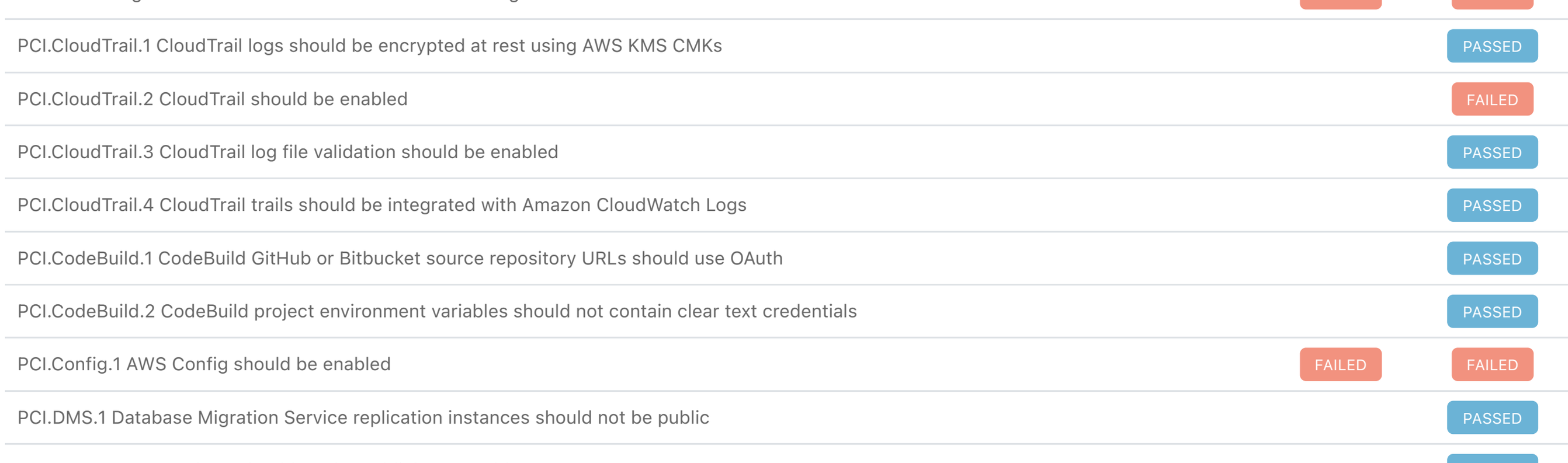
Findings by severity
The chart below shows the high level severity of the findings for this security standard



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