Qualys TotalCloud

Policy Document

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100

Table of Contents

CIS Amazon Web Services Foundations Benchmark v3.0.0

Control ID - 1: Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password.

Control ID - 2: Ensure console credentials unused for 45 days or greater are disabled.

Control ID - 4: Ensure access key1 is rotated every 90 days or less.

Control ID - 5: Ensure access key2 is rotated every 90 days or less.

Control ID - 11: Ensure IAM password policy requires minimum length of 14 or greater

Control ID - 12: Ensure IAM password policy prevents password reuse.

Control ID - 14: Ensure no root user account access key exists.

Control ID - 15: Ensure MFA is enabled for the root user account

Control ID - 16: Ensure hardware MFA is enabled for the root account

Control ID - 18: Eliminate use of the root user for administrative and daily tasks.

Control ID - 19: Ensure CloudTrail is enabled in all regions.

Control ID - 20: Ensure CloudTrail log file validation is enabled.

Control ID - 23: Ensure AWS Config is enabled in all regions.

Control ID - 24: Ensure S3 bucket access logging is enabled on the CloudTrail S3 bucket.

Control ID - 25: Ensure CloudTrail logs are encrypted at rest using KMS CMKs.

Control ID - 26: Ensure rotation for customer created symmetric CMKs is enabled.

Control ID - 27: Ensure unauthorized API calls are monitored.

Control ID - 28: Ensure management console sign-in without MFA is monitored.

Control ID - 29: Ensure usage of root account is monitored.

Control ID - 30: Ensure IAM policy changes are monitored.

Control ID - 31: Ensure CloudTrail configuration changes are monitored.

Control ID - 32: Ensure AWS Management Console authentication failures are monitored.

Control ID - 33: Ensure disabling or scheduled deletion of customer created CMKs is monitored.

Control ID - 34: Ensure S3 bucket policy changes are monitored.

Control ID - 35: Ensure AWS Config configuration changes are monitored.

Control ID - 36: Ensure security group changes are monitored.

Control ID - 37: Ensure Network Access Control Lists (NACL) changes are monitored.

Control ID - 38: Ensure changes to network gateways are monitored.

Control ID - 39: Ensure route table changes are monitored.

Control ID - 40: Ensure VPC changes are monitored.

Control ID - 41: Ensure no security groups allow ingress from 0.0.0.0/0 to port 22.

Control ID - 42: Ensure no security groups allow ingress from 0.0.0.0/0 to port 3389.

Control ID - 43: Ensure VPC flow logging is enabled in all VPCs.

Control ID - 44: Ensure the default security group of every VPC restricts all traffic.

Control ID - 49: Ensure a support role has been created to manage incidents with AWS Support

Control ID - 50: Ensure IAM policies that allow full *:* administrative privileges are not attached.

Control ID - 53: Ensure that encryption-at-rest is enabled for RDS Instances.

Control ID - 55: Ensure Auto Minor Version Upgrade feature is Enabled for RDS Instances.

Control ID - 57: Ensure S3 Bucket Policy is set to deny HTTP requests.

Control ID - 59: Ensure Block new public bucket policies for a bucket is set to true.

Control ID - 60: Ensure that Block public and cross-account access if bucket has public policies for bucket is set to true

Control ID - 61: Ensure that Block new public ACLs and uploading public objects for a bucket is set to true.

Control ID - 62: Ensure that Remove public access granted through public ACLs for a bucket is set to true.

Control ID - 68: Ensure all the expired SSL/TLS certificates stored in AWS IAM are removed.

Control ID - 78: Ensure that public access is not given to RDS Instance.

Control ID - 115: Ensure that EBS Volumes attached to EC2 instances are encrypted.

Control ID - 116: Ensure that Unattached EBS Volumes are encrypted.

Control ID - 144: Ensure EFS Encryption is enabled for data at rest

Control ID - 160: Ensure that IAM Access analyzer is enabled for all regions.

Control ID - 161: Ensure no Network ACLs allow ingress from 0.0.0.0/0 to port 22.

Control ID - 170: Ensure no Network ACLs allow ingress from 0.0.0.0/0 to port 3389.

Control ID - 171: Ensure there is only one active access key available for any single IAM user.

Control ID - 172: Ensure AWS Organizations changes are monitored.

Control ID - 175: Ensure no Inline Policies are attached to IAM Users directly.

Control ID - 176: Ensure no Managed Policies are attached to IAM Users directly.

Control ID - 177: Ensure that Object-level logging for write events is enabled for S3 bucket.

Control ID - 178: Ensure that Object-level logging for read events is enabled for S3 bucket.

Control ID - 199: Ensure not to setup access keys during initial user setup for all IAM users that have a console password except for the master account

Control ID - 253: Ensure AWS Security Hub is enabled in all regions.

Control ID - 255: Ensure MFA Delete is enabled on S3 buckets.

Control ID - 433: Ensure IAM instance roles are used for AWS resource access from instances

AWS Lambda Best Practices Policy

Control ID - 97: Ensure that Lambda function has tracing enabled

Control ID - 98: Ensure that Lambda Function is not using An IAM role for more than one Lambda Function

Control ID - 99: Ensure that Multiple Triggers are not configured in $Latest Lambda Function

Control ID - 100: Ensure that Lambda Runtime Version is latest and not custom

Control ID - 101: Ensure that Lambda function does not have Admin Privileges

Control ID - 102: Ensure that Lambda function does not have Cross Account Access

Control ID - 103: Ensure that Lambda Environment Variables at-rest are encrypted with CMK

Control ID - 104: Ensure that Lambda Environment Variables are encrypted using AWS encryption helpers for encryption in transit

Control ID - 105: Ensure that Lambda function does not allows anonymous invocation

Control ID - 106: Ensure that VPC access for Lambda Function is not set to default(Null)

Control ID - 107: Ensure that AWS Lambda excess Permissions are removed

Control ID - 125: Ensure that multiple triggers are not configured for Lambda Function Aliases

Control ID - 343: Ensure that AWS Lambda function is configured for function-level concurrent execution limit

Control ID - 344: Ensure that AWS Lambda function is configured for a Dead Letter Queue(DLQ)

Control ID - 442: Ensure that your Amazon Lambda functions are configured to use enhanced monitoring

AWS Database Service Best Practices

Control ID - 51: Ensure that Public Accessibility is set to No for Database Instances

Control ID - 52: Ensure DB snapshot is not publicly visible

Control ID - 54: Ensure database Instance snapshot is encrypted

Control ID - 56: Ensure database Instance is not listening on to a standard/default port

Control ID - 69: Ensure automated backups are enabled for RDS database instances

Control ID - 70: Ensure Deletion Protection is enabled for RDS DB Cluster

Control ID - 71: Ensure Deletion Protection is enabled for RDS Database instances

Control ID - 72: Ensure IAM Database Authentication is Enabled for the DB Cluster

Control ID - 73: Ensure IAM Database Authentication is Enabled for the DB Instances

Control ID - 74: Ensure AWS RDS Log Exports is enabled for DB Cluster

Control ID - 75: Ensure AWS RDS Log Exports is enabled for DB Instances

Control ID - 76: Ensure RDS Database Master username is not set to well-known/default

Control ID - 77: Ensure VPC security group attached to RDS Database Instance does not allows Inbound traffic from ANY source IP

Control ID - 79: Ensure RDS DB Cluster are not present in public subnets

Control ID - 80: Ensure Event Subscriptions for Instance Level Events is Enabled for DB Instances

Control ID - 81: Ensure RDS Microsoft SQL instance enforces encrypted connections only

Control ID - 82: Ensure RDS PostgreSQL instance enforces encrypted connections only

Control ID - 83: Ensure RDS PostgreSQL Cluster enforces encrypted connections only

Control ID - 84: Ensure Encryption is enabled for the RDS DB Cluster

Control ID - 85: Ensure RDS DB Cluster snapshots are encrypted

Control ID - 86: Ensure CMK is used to protect RDS DB Cluster encryption key

Control ID - 87: Ensure CMK is used to protect RDS Db Instance encryption key

Control ID - 88: Ensure DB instance replication is set to the another Zone for High Availability

Control ID - 89: Ensure DB Cluster replication is set to the another Zone for High Availability

Control ID - 90: Ensure RDS database Cluster snapshots are not public

Control ID - 91: Ensure Enhance monitoring is enabled for RDS Database Instance

Control ID - 92: Ensure AWS RDS DB Cluster with copy tags to snapshots option is enabled

Control ID - 93: Ensure AWS RDS instances with copy tags to snapshots option is enabled

Control ID - 94: Ensure Event Subscriptions for cluster Level Events is Enabled for DB Clusters

Control ID - 95: Ensure MYSQL DB Instance backup Binary logs configuration is not set to OFF

Control ID - 96: Ensure backup configuration is enabled for MSSQL DB Instances

Control ID - 108: Ensure Version Upgrade is enabled for AWS Redshift clusters to automatically receive upgrades

Control ID - 109: Ensure AWS Redshift clusters are not using default endpoint port

Control ID - 110: Ensure AWS Redshift clusters are not publicly accessible

Control ID - 111: Ensure AWS Redshift clusters master username is not set to well-known/default

Control ID - 112: Ensure that AWS Redshift clusters encryption is set for data at rest

Control ID - 113: Ensure audit logging is enabled for AWS Redshift clusters for security and troubleshooting purposes

Control ID - 117: Ensure that RDS Instances certificates are rotated

Control ID - 118: Ensure that DocumentDB Instances certificates are rotated

Control ID - 132: Ensure DocumentDB database cluster master username is not set to well-known/default

Control ID - 133: Ensure backup retention is set to minimum of 7 days for DocumentDB clusters

Control ID - 134: Ensure audit logs is enabled for Log export to CloudWatch for DocumentDB clusters

Control ID - 135: Ensure deletion protection is enabled for DocumentDB clusters

Control ID - 136: Ensure DocumentDB Cluster is not listening on default port

Control ID - 137: Ensure multi-AZ high availability is enabled for neptune DB

Control ID - 138: Ensure neptune DB is not listening on default port

Control ID - 139: Ensure IAM DB authentication is enabled for neptune database

Control ID - 140: Ensure backup retention is set to minimum of 7 days for neptune database

Control ID - 141: Ensure Audit logs is enabled for log exports to cloudwatch for neptune database

Control ID - 142: Ensure Auto minor version upgrade is enabled for neptune database

Control ID - 143: Ensure deletion protection is enabled for neptune DB

Control ID - 169: Ensure DynamoDB tables are encrypted using KMS Customer managed Keys

Control ID - 173: Ensure DynamoDB tables are not configured using DEFAULT encryption

Control ID - 180: Ensure QLDB ledger has deletion protection enabled

Control ID - 189: Ensure Automated backup retention is set for Redshift Cluster

Control ID - 190: Ensure Redshift Cluster is configured to require an SSL connection

Control ID - 191: Ensure database audit logging is enabled for Redshift Cluster

Control ID - 192: Ensure Redshift Cluster is encrypted with KMS key

Control ID - 201: Ensure RDS Instance should not have an Interface open to a public scope

Control ID - 206: Ensure that DocumentDB Cluster Snapshots are encrypted

Control ID - 207: Ensure that DocumentDB Cluster Snapshots are not public

Control ID - 219: Ensure neptune DB snapshots are encrypted

Control ID - 220: Ensure neptune DB snapshots are not public

Control ID - 250: Ensure AWS RDS instance is not open to a large scope

Control ID - 251: Ensure QLDB ledger has encryption enabled using accessible Customer managed KMS key

Control ID - 254: Ensure that backup retention is set between 3 to 7 days for Aurora postgreSQL clusters

Control ID - 257: Ensure status of the log_destination parameter for PostgreSQL instance is set to csvlog

Control ID - 258: Ensure status of the log_rotation_age parameter for PostgreSQL instance is set to 60(minutes)

Control ID - 259: Ensure status of the log_connections parameter for PostgreSQL instance is set to ON(1)

Control ID - 260: Ensure status of the log_disconnections parameter for PostgreSQL instance is set to ON(1)

Control ID - 261: Ensure status of the log_hostname parameter for PostgreSQL instance is set to OFF(0)

Control ID - 262: Ensure status of the log_statement parameter for PostgreSQL instance is set to ddl or stricter

Control ID - 263: Ensure status of the pgaudit.log parameter for PostgreSQL instance is set to appropriate value

Control ID - 265: Ensure status of the log_destination parameter for Aurora PostgreSQL cluster is set to csvlog

Control ID - 266: Ensure status of the log_rotation_age parameter for Aurora PostgreSQL cluster is set to 60(minutes)

Control ID - 267: Ensure status of the log_connections parameter for Aurora PostgreSQL cluster is set to ON(1)

Control ID - 268: Ensure status of the log_disconnections parameter for Aurora PostgreSQL cluster is set to ON(1)

Control ID - 269: Ensure status of the log_hostname parameter for Aurora PostgreSQL cluster is set to OFF(0)

Control ID - 270: Ensure status of the log_statement parameter for Aurora PostgreSQL cluster is set to ddl or stricter

Control ID - 271: Ensure status of the pgaudit.log parameter for Aurora PostgreSQL cluster is set to appropriate value

Control ID - 292: Ensure Dynamodb point in time recovery (backup) is enabled

Control ID - 302: Ensure DAX is encrypted at rest (default is unencrypted)

Control ID - 330: Ensure DocDB TLS is not disabled

Control ID - 333: Ensure all data stored in Aurora is securely encrypted at rest

Control ID - 371: Ensure Redshift is not deployed outside of a VPC

Control ID - 384: Ensure QLDB ledger permissions mode is set to STANDARD

Control ID - 393: Ensure the option group attached to the RDS Oracle Instance have TLSv1.2 and the required ciphers configured

Control ID - 402: Ensure that PostgreSQL RDS instances have Query Logging enabled

Control ID - 409: Ensure that ssl_max_protocol_version parameter for Aurora PostgreSQL cluster is set to latest version

Control ID - 410: Ensure that ssl_min_protocol_version parameter for Aurora PostgreSQL cluster is set to latest version

Control ID - 413: Ensure that your Amazon Relational Database Service (RDS) instances have Storage AutoScaling feature enabled

Control ID - 432: Ensure that your Amazon DynamoDB tables are using backup and restore

Control ID - 435: Ensure Performance Insights feature is enabled for your Amazon RDS database instances

Control ID - 455: Ensure backtracking is enabled for AWS RDS cluster

Control ID - 456: Ensure database retention is set to 7 days or more for AWS RDS cluster

Control ID - 457: Ensure Aurora Serverless AutoPause is enabled for RDS cluster

Control ID - 459: Ensure Enhanced VPC routing should be enabled for AWS Redshift Clusters

Control ID- 507: Ensure encryption at rest is enabled for AWS DocumentDB clusters

Control ID- 512: Ensure storage encryption is enabled for AWS Neptune cluster

Control ID - 530: Ensure that encryption is enabled for AWS Neptune instances

Control ID - 531: Ensure that your Amazon Neptune database instances are using KMS Customer Master Keys (CMKs)

AWS Best Practices Policy

Control ID - 3: Ensure access keys unused for 90 days or greater are disabled

Control ID - 6: Ensure IAM Password Policy is Enabled

Control ID - 7: Ensure IAM password policy requires at least one uppercase letter

Control ID - 8: Ensure IAM password policy require at least one lowercase letter

Control ID - 9: Ensure IAM password policy require at least one symbol

Control ID - 10: Ensure IAM password policy require at least one number

Control ID - 13: Ensure IAM password policy expires passwords within 90 days or less

Control ID - 17: Ensure IAM policies are attached only to groups or roles

Control ID - 21: Ensure the S3 bucket used to store CloudTrail logs is not publicly accessible.

Control ID - 22: Ensure CloudTrail trails are integrated with CloudWatch Logs.

Control ID - 45: S3 Bucket Access Control List Grant Access to Everyone or Authenticated Users

Control ID - 46: S3 Bucket Policy Grant Access to Everyone

Control ID - 47: Ensure access logging is enabled for S3 buckets

Control ID - 48: Ensure versioning is enabled for S3 buckets

Control ID - 58: Ensure that the key expiry is set for CMK with external key material

Control ID - 63: Ensure Block new public bucket policies for an account is set to true

Control ID - 64: Ensure that Block public and cross-account access if bucket has public policies for the account is set to true

Control ID - 65: Ensure that Block new public ACLs and uploading public objects for the account is set to true

Control ID – 67: Ensure all S3 buckets employ encryption-at-rest

Control ID - 66: Ensure that Remove public access granted through public ACLs for the account is enabled

Control ID - 114: Ensure Images (AMIs) owned by an AWS account are not public

Control ID - 119: Ensure no AWS default KMS Key is used to protect Secrets

Control ID - 120: Ensure No CMK is marked for deletion

Control ID - 121: Ensure only Root user of the AWS Account should be allowed full access on the CMK

Control ID - 122: Permissions to delete key is not granted to any Principal other than the Root user of AWS Account

Control ID - 123: Ensure CMK administrators are not the user of the key

Control ID - 124: Ensure all Custom key stores are connected to their CloudHSM clusters

Control ID - 126: Ensure AMIs owned by an AWS account are encrypted

Control ID - 127: Ensure AWS EBS Volume snapshots are encrypted

Control ID - 128: Ensure access log is enabled for Application load balancer

Control ID - 129: Ensure access log is enabled for Classic Elastic load balancer

Control ID - 130: Ensure Classic Elastic load balancer is not using unencrypted protocol

Control ID - 131: Ensure Elastic load balancer listener is not using unencrypted protocol

Control ID - 145: Ensure EFS File system resource is encrypted by KMS using a customer managed Key (CMK)

Control ID - 146: Ensure that AWS Elastic Block Store (EBS) volume snapshots are not public

Control ID - 147: Ensure that AWS ElastiCache Memcached clusters are not associated with default VPC

Control ID - 148: Ensure that AWS ElastiCache Redis clusters are not associated with default VPC

Control ID - 149: Ensure that AWS ElastiCache redis clusters are not using their default endpoint ports

Control ID - 150: Ensure that AWS ElastiCache memcached clusters are not using their default endpoint ports

Control ID - 151: Ensure AWS ElastiCache Redis cluster with Multi-AZ Automatic Failover feature is set to enabled

Control ID - 152: Ensure AWS ElastiCache Redis cluster with Redis AUTH feature is enabled

Control ID - 153: Ensure that AWS ElastiCache Redis clusters are In-Transit encrypted

Control ID - 154: Ensure that AWS ElastiCache Redis clusters are Data At-Rest encrypted

Control ID - 155: Ensure that AWS ElastiCache Redis clusters are Data At-Rest encrypted with CMK

Control ID - 156: Ensure node-to-node encryption feature is enabled for AWS Elasticsearch Service domains

Control ID - 157: Ensure AWS Elasticsearch Service domains have enabled the support for publishing slow logs to AWS CloudWatch Logs

Control ID - 158: Ensure AWS Elasticsearch Service domains are not publicly accessible

Control ID - 159: Ensure AWS Elasticsearch Service domains are using the latest version of Elasticsearch engine

Control ID - 162: Ensure AWS Route 53 Registered domain has Transfer lock enabled

Control ID - 163: Ensure AWS Route 53 Registered domain has Auto renew Enabled

Control ID - 164: Ensure AWS Route 53 Registered domain is not expired

Control ID - 165: Ensure AWS Kinesis Data Firehose delivery stream with Direct PUT and other sources as source has Server-side encryption configured

Control ID - 166: Ensure AWS Kinesis Data Firehose delivery stream with Kinesis Data stream as source has Server-side encryption configured

Control ID - 167: Ensure AWS Kinesis Data Firehose delivery stream with Direct PUT and other sources as source has Server-side encryption configured with KMS Customer Managed Keys

Control ID - 168: Ensure AWS Kinesis Data Firehose delivery stream with Kinesis Data stream as source has Server-side encryption configured with KMS Customer Managed Keys

Control ID - 174: Ensure that Customer managed KMS keys use external key material

Control ID - 179: Ensure MFA is enabled in AWS Directory

Control ID - 181: Ensure proper protocol is configured for Radius server in AWS Directory

Control ID - 182: Ensure SNS Topics do not Allow Everyone to Publish

Control ID - 183: Ensure SNS Topics do not Allow Everyone to Subscribe

Control ID - 184: Ensure there are no Internet facing Application load balancers

Control ID - 185: Ensure ALB using listener type HTTPS must have SSL Security Policy

Control ID - 186: Ensure that ALB using listener type HTTP must be redirected to HTTPS

Control ID - 187: Ensure that ALB listeners have HTTPS enabled Target Groups

Control ID - 188: Ensure IncreaseVolumeSize is Disabled for Workspace directories in all regions

Control ID - 193: Ensure that NLB balancer listener is not using unencrypted protocol

Control ID - 194: Ensure that Classic Elastic load balancer is not internet facing

Control ID - 195: Ensure Classic Elastic Load balancer must have SSL Security Policy

Control ID - 196: Ensure AWS VPC subnets have automatic public IP assignment disabled

Control ID - 197: Ensure to encrypt the User Volumes and Root Volumes with the customer managed master keys for AWS WorkSpace

Control ID - 198: Ensure Workspace directory must have a vpc endpoint so that the API traffic associated with the management of workspaces stays within the vpc

Control ID - 200: Ensure to log state machine execution history to CloudWatch Logs

Control ID - 202: Ensure to update the Security Policy of the Network Load Balancer

Control ID - 203: Ensure EBS Volume is encrypted by KMS using a customer managed Key (CMK)

Control ID - 204: Ensure AWS EBS Volume snapshots are encrypted with KMS using a customer managed Key (CMK)

Control ID - 205: Ensure RestartWorkspace is Enabled for Directories in all regions

Control ID - 208: Ensure WorkDocs is not enabled in Workspace Directories

Control ID - 209: Ensure Access to Internet is not enabled in Workspace Directories

Control ID - 210: Ensure Local Administrator setting is not enabled in Workspace Directories

Control ID - 211: Ensure Maintenance Mode is not enabled in Workspace Directories

Control ID - 212: Ensure Device Type Windows Access Control is allowed in Workspace Directories

Control ID - 213: Ensure Device Type MacOS Access Control is allowed in Workspace Directories

Control ID - 214: Ensure Device Type Web Access Control is allowed in Workspace Directories

Control ID - 215: Ensure Device Type iOS Access Control is allowed in Workspace Directories

Control ID - 216: Ensure Device Type Android Access Control is allowed in Workspace Directories

Control ID - 217: Ensure Device Type ChromeOS Access Control is allowed in Workspace Directories

Control ID - 218: Ensure Device Type ZeroClient Access Control is allowed in Workspace Directories

Control ID - 221: Ensure ChangeComputeType is Disabled in all regions for Workspace Directories

Control ID - 222: Ensure SwitchRunningMode is Disabled in all regions for Workspace Directories

Control ID - 223: Ensure RebuildWorkspace is Disabled in all regions for Workspace Directories

Control ID - 224: Ensure only AD Connector directory type is allowed for AWS Directories

Control ID - 225: Ensure to enable the encryption of the Root volumes for Workspaces in all regions

Control ID - 226: Ensure to enable the encryption of the User volumes for Workspaces in all regions

Control ID - 227: Ensure Amazon API Gateway APIs are only accessible through private API endpoints in all regions

Control ID - 228: Ensure to disable default route table association for Transit Gateways in all regions

Control ID - 229: Ensure to disable default route table propagation for Transit Gateways in all regions

Control ID - 230: Ensure to enable config for the all resources for Config Service

Control ID - 231: Ensure to enable config for the global resources like IAM for Config Service

Control ID - 232: Ensure to configure data retention period for the configuration items for Config Service

Control ID - 233: Ensure to configure s3 buckets which contains details for the resources that Config records

Control ID - 234: Ensure to configure certificate provider type to custom in EMR security configuration

Control ID - 235: Ensure to enable data in transit encryption for EMR security configuration

Control ID - 236: Ensure that all AWS Systems Manager (SSM) parameters are encrypted

Control ID - 237: Ensure termination protection is enabled for EMR cluster

Control ID - 238: Ensure ACM uses imported certificates only and does not create/issue certificates

Control ID - 239: Ensure expired certificates are removed from AWS ACM

Control ID - 240: Ensure ACM certificates should not have domain with wildcard(*)

Control ID - 241: Ensure that the certificate use appropriate algorithms and key size

Control ID - 242: Ensure logging is not set to OFF for Rest APIs Stage in all regions

Control ID - 243: Ensure to enable encryption if caching is enabled for Rest API Stage in all regions

Control ID - 244: Ensure accessLogSettings exists with the destinationArn and in the json format for Rest API Stage in all regions

Control ID - 245: Ensure there are no Internet facing Network load balancers

Control ID - 246: Ensure NLB using listener type TLS must have SSL Security Policy

Control ID - 247: Ensure that NLB listeners using TLS have TLS enabled Target Groups configured

Control ID - 248: Ensure that NLB listeners using default insecure ports are not configured for passthrough

Control ID - 249: Ensure AWS NLB logging is enabled

Control ID - 252: Ensure to encrypt the data in transit when using NFS between the client and EFS service

Control ID - 256: Ensure trail is configure on organization level

Control ID - 264: Ensure each trail includes the global services

Control ID - 272: Ensure to log KMS events to the trail

Control ID - 273: Ensure block public access is enabled so that no port should have public access for EMR clusters

Control ID - 285: Ensure all data stored in the Elasticsearch is securely encrypted at rest

Control ID - 286: Ensure all data stored in the Launch configuration EBS is securely encrypted

Control ID - 288: Ensure SageMaker Notebook is encrypted at rest using KMS CMK

Control ID - 289: Ensure every security groups rule has a description

Control ID - 290: Ensure SNS Topics have encryption at rest enabled

Control ID - 291: Ensure SQS Queue have encryption at rest enabled

Control ID - 293: Ensure ECR repository policy is not set to public

Control ID - 294: Ensure Customer managed KMS key policy does not contain wildcard (*) principal

Control ID - 295: Ensure Cloudfront distribution ViewerProtocolPolicy is set to HTTPS

Control ID - 303: Ensure MQ Broker logging is enabled

Control ID - 305: Ensure ECR Image Tags are immutable

Control ID - 312: Ensure container insights are enabled on ECS cluster

Control ID - 314: Ensure that CloudFront Distribution has WAF enabled

Control ID - 315: Ensure MQ Broker is not publicly exposed

Control ID - 318: Ensure API Gateway has X-Ray Tracing enabled

Control ID - 319: Ensure Global Accelerator has flow logs enabled

Control ID - 321: Ensure that CodeBuild Project encryption is not disabled

Control ID - 322: Ensure Instance Metadata Service Version 2 is Enabled

Control ID - 323: Ensure MSK Cluster logging is enabled

Control ID - 324: Ensure MSK Cluster encryption at rest and in transit is enabled

Control ID - 325: Ensure Athena Workgroups enforce configuration to prevent client disabling encryption

Control ID - 326: Ensure Elasticsearch Domain enforces HTTPS

Control ID - 327: Ensure Cloudfront distribution has Access Logging enabled

Control ID - 328: Ensure that EC2 instance have no public IP

Control ID - 329: Ensure that DMS replication instance is not publicly accessible

Control ID - 332: Ensure Glue Data Catalog Encryption is enabled with SSE-KMS with customer-managed keys

Control ID - 334: Ensure all data stored in the Sagemaker Endpoint is securely encrypted at rest

Control ID - 338: Ensure that load balancer is using TLS 1.2 or above

Control ID - 339: Ensure EBS default encryption is enabled with customer managed key

Control ID - 342: Ensure that EMR clusters with Kerberos have Kerberos Realm set

Control ID - 346: Ensure network load balancers should have security group attached

Control ID - 347: Ensure that direct internet access is disabled for an Amazon SageMaker Notebook Instance

Control ID - 348: Ensure that VPC Endpoint Service is configured for Manual Acceptance

Control ID - 349: Ensure that CloudFormation stacks are sending event notifications to an SNS topic

Control ID - 350: Ensure that detailed monitoring is enabled for EC2 instances

Control ID - 351: Ensure that Elastic Load Balancers use SSL certificates provided by AWS Certificate Manager

Control ID - 354: Ensure that ALB drops HTTP headers

Control ID - 355: Ensure Trail is configured to log Data events for s3 buckets

Control ID - 357: Ensure that EC2 is EBS optimized

Control ID - 358: Ensure that ECR repositories are encrypted using KMS

Control ID - 359: Ensure that Elasticsearch is configured inside a VPC

Control ID - 360: Ensure that ELB has cross-zone-load-balancing enabled

Control ID - 366: Ensure that Secrets Manager secret is encrypted using KMS using a customer managed Key (CMK)

Control ID - 367: Ensure that Load Balancer has deletion protection enabled

Control ID - 369: Ensure that Load Balancer (Network/Gateway) has cross-zone load balancing enabled

Control ID - 370: Ensure that Auto Scaling Groups supply tags to Launch Configurations

Control ID - 373: Ensure to encrypt CloudWatch log groups

Control ID - 374: Ensure that Athena Workgroup is encrypted

Control ID - 377: Ensure ECR image scanning on push is enabled

Control ID - 378: Ensure Transfer Server is not exposed publicly.

Control ID - 379: Ensure S3 bucket must not allow WRITE permission for server access logs from everyone on the bucket

Control ID - 380: Ensure Backup Vault is encrypted at rest using KMS CMK

Control ID - 381: Ensure Glacier Vault access policy is not public by only allowing specific services or principals to access it

Control ID - 382: Ensure SQS queue policy is not public by only allowing specific services or principals to access it

Control ID - 383: Ensure SNS topic policy is not public by only allowing specific services or principals to access it

Control ID - 385: Ensure that EMR Cluster security configuration encryption is using SSE-KMS

Control ID - 386: Ensure that all NACLs are attached to subnets

Control ID - 387: Ensure GuardDuty is enabled to specific org/region

Control ID - 388: Ensure API Gateway stage have logging level defined as appropriate and have metrics enabled

Control ID - 395: Ensure that Auto Scaling Groups that are associated with a Load Balancer are using Elastic Load Balancing health checks

Control ID - 396: Ensure that Auto Scaling is enabled on your DynamoDB tables

Control ID - 398: Ensure that all EIP addresses allocated to a VPC are attached to EC2 instances

Control ID - 399: Ensure that all IAM users are members of at least one IAM group.

Control ID - 400: Ensure an IAM User does not have access to the console

Control ID - 401: Route53 A Record has Attached Resource

Control ID - 403: Ensure public facing ALB are protected by WAF

Control ID - 407: Ensure all data stored in the Elasticache Replication Group is securely encrypted at transit and has auth token

Control ID - 411: Ensure that a log driver has been defined for each active Amazon ECS task definition

Control ID - 419: Ensure that AWS CloudFront distribution origins do not use insecure SSL protocols

Control ID - 426: Ensure Amazon API Gateway REST APIs are protected by AWS WAF

Control ID - 427: Ensure client-side SSL certificates are used for HTTP backend authentication in AWS API Gateway REST APIs

Control ID - 428: Ensure that SSL certificates associated with API Gateway REST APIs are rotated periodically

Control ID - 429: Ensure AWS CloudFront distributions use improved security policies for HTTPS connections

Control ID - 430: Ensure the traffic between the AWS CloudFront distributions and their origins is encrypted

Control ID - 431: Ensure your AWS Cloudfront distributions are using an origin access identity for their origin S3 buckets

Control ID - 436: Ensure to encrypt data in transit for SNS topic

Control ID - 437: Ensure unused AWS EC2 key pairs are decommissioned

Control ID - 438: Ensure AWS SNS topics do not allow HTTP subscriptions

Control ID - 439: Ensure that Elastic File System does not have the default access policy

Control ID - 440: Ensure that the latest version of Memcached is used for AWS ElastiCache clusters

Control ID - 443: Ensure that Route 53 Hosted Zone has configured logging for DNS queries

Control ID - 444: Ensure that DNSSEC Signing is enabled for Route 53 Hosted Zones

Control ID - 445: Ensure that Route 53 domains have Privacy Protection enabled

Control ID - 446: Ensure a loggroup is created to upload logs of datasync task to the cloudwatch log group

Control ID - 447: Ensure to enable data integrity checks for only files transferred in datasync task

Control ID - 448: Ensure that all your SSL/TLS IAM certificates are using 2048 or higher bit RSA keys

Control ID - 449: Ensure to disable default endpoint for all the APIs

Control ID - 450: Ensure that Microsoft AD directory forward domain controller security event logs to cloudwatch logs

Control ID - 451: Ensure SQS queues uses KMS customer managed master key

Control ID - 452: Ensure SQS queues are encrypted in transit

Control ID - 453: Ensure to block public access to Amazon EFS file systems

Control ID - 458: Ensure connection draining is enabled for AWS ELB

Control ID - 460: Ensure that content encoding is enabled for API Gateway Rest API

Control ID - 461: Ensure to configure idle session timeout in all regions

Control ID - 462: Ensure session logs for system manager are stored in CloudWatch log groups or S3 buckets

Control ID - 463: Ensure session logs for system manager are stored in only Encrypted CloudWatch log groups or S3 buckets

Control ID - 464: Ensure Block public sharing setting is ON for the documents in all regions

Control ID - 465: Ensure stage caching is enabled for AWS API Gateway Method Settings

Control ID - 466: Ensure transit encryption is enabled for EFS volumes in AWS ECS Task Definition

Control ID - 467: Ensure to disable root access for all notebook instance users

Control ID - 468: Ensure to enable inter-container traffic encryption for Processing jobs(if configured)

Control ID - 469: Ensure processing jobs(if configured) are running inside a VPC

Control ID - 470: Ensure to enable network isolation for processing jobs(if configured)

Control ID - 471: Ensure ML storage volume attached to training jobs are encrypted

Control ID - 472: Ensure ML storage volume attached to training jobs are encrypted with customer managed master key

Control ID - 473: Ensure to encrypt the output of the training jobs in s3 with customer managed master key

Control ID - 474: Ensure to enable inter-container traffic encryption for training jobs

Control ID - 475: Ensure to enable network isolation for training jobs

Control ID - 476: Ensure ML storage volume attached to Hyperparameter Tuning jobs are encrypted

Control ID - 477: Ensure ML storage volume attached to Hyperparameter Tuning jobs (if configured) are encrypted with customer managed master key

Control ID - 478: Ensure to encrypt the output of Hyperparameter tuning jobs in s3

Control ID - 479: Ensure to encrypt the output of Hyperparameter tuning jobs(if configured) in s3 with customer managed master key

Control ID - 480: Ensure to enable inter-container traffic encryption for Hyperparameter tuning jobs(if configured)

Control ID - 481: Ensure Hyperparameter tuning jobs(if configured) are running inside a VPC

Control ID - 482: Ensure to enable network isolation for Hyperparameter tuning jobs(if configured)

Control ID - 483: Ensure to enable network isolation for models

Control ID - 485: Ensure to enable CloudWatch logging in the audit logging account

Control ID - 489: Ensure multi-az is enabled for AWS DMS instances

Control ID - 490: Ensure auto minor version upgrade is enabled for AWS DMS instances

Control ID - 491: Ensure auto minor version upgrade is enabled for AWS MQ Brokers

Control ID - 492: Ensure active/standby deployment mode is used for AWS MQ Brokers

Control ID - 495: Ensure advanced security options are enabled for AWS ElasticSearch Domain

Control ID - 496: Ensure general purpose SSD node type is used for AWS ElasticSearch Domains

Control ID - 497: Ensure KMS customer managed keys are used for encryption for AWS ElasticSearch Domains

Control ID - 498: Ensure Zone Awareness is enabled for AWS ElasticSearch Domain

Control ID - 499: Ensure Amazon cognito authentication is enabled for AWS ElasticSearch Domain

Control ID - 500: Ensure dedicated master nodes are enabled for AWS ElasticSearch Domains

Control ID - 501: Ensure policies are used for AWS CloudFormation Stacks

Control ID - 502: Ensure termination protection is enabled for AWS CloudFormation Stack

Control ID - 503: Ensure TLS security policy is using 1.2 version for the custom domains

Control ID - 504: Ensure there is a Dead Letter Queue configured for each Amazon SQS queue

Control ID - 505: Ensure that EMR cluster is configured with security configuration

Control ID - 506: Ensure AWS Elastic MapReduce (EMR) clusters capture detailed log data to Amazon S3

Control ID - 508: Ensure AWS EBS Volume has a corresponding AWS EBS Snapshot

Control ID - 509: Ensure egress filter is set as DROP_ALL for AWS Application Mesh

Control ID - 510: Ensure secrets should be auto rotated after not more than 90 days

Control ID - 511: Ensure CORS is configured to prevent sharing across all domains for AWS API Gateway V2 API

Control ID- 514: Ensure sufficient data retention period is set for AWS Kinesis Streams (7 days or More)

Control ID - 516: Ensure AWS ACM certificates are renewed 7 days before expiration date

Control ID- 517: Ensure customer master key (CMK) is not disabled for AWS Key Management Service (KMS)

Control ID - 518: Ensure SNS Topics are encrypted with customer managed master key

Control ID - 519: Ensure ML storage volume attached to notebooks are encrypted

Control ID - 520: Ensure ML storage volume attached to notebooks are encrypted with customer managed master key

Control ID - 521: Ensure ML storage volume attached to processing jobs are encrypted

Control ID - 522: Ensure ML storage volume attached to processing jobs(if configured) are encrypted with customer managed master key

Control ID - 523: Ensure to encrypt the output of processing jobs

Control ID - 524: Ensure to encrypt the output of processing jobs(if configured)in s3 with customer managed master key

Control ID - 527: Ensure to encrypt the destination bucket in s3 in the audit logging account

Control ID - 528: Ensure to encrypt the destination bucket in s3 with customer managed master keys in the audit logging account

Control ID - 529: Ensure detailed monitoring is enabled for AWS Launch Configuration

Control ID - 533: Ensure that ACM Certificate is validated

CIS Microsoft Azure Foundations Benchmark v2.1.0

Control ID - 50001: Ensure that Data encryption is set to ON for a SQL database.

Control ID - 50002: Ensure no SQL Servers allow ingress from Internet (ANY IP)

Control ID - 50004: Ensure that Auto provisioning of Log Analytics agent for Azure VMs is set to On.

Control ID - 50005: Ensure that Microsoft Defender Recommendation for Apply system updates status is Completed

Control ID - 50008: Ensure that Disk encryption should be applied on virtual machines is set to On.

Control ID - 50011: Ensure that Secure transfer required is set to Enabled.

Control ID - 50015: Ensure that Microsoft Defender for Servers is set to On.

Control ID - 50016: Ensure that Access through Internet facing endpoint should be restricted is set to On.

Control ID - 50020: Ensure Additional email addresses is configured with a security contact email

Control ID - 50022: Ensure that Notify about alerts with the following severity is set to High.

Control ID - 50023: Ensure that All users with the following roles is set to Owner.

Control ID - 50026: Ensure keyvault is recoverable.

Control ID - 50027: Ensure SQL server Transparent Data Encryption (TDE) protector is encrypted with Customer-managed key

Control ID - 50029: Disable RDP access on Network Security Groups from Internet (ANY IP)

Control ID - 50030: Ensure that the Expiration Date is set for all Secrets in Non RBAC Key Vaults.

Control ID - 50031: Disable SSH access on Network Security Groups from Internet (ANY IP)

Control ID - 50032: Ensure that Unattached disks are encrypted with Customer Managed Key (CMK)

Control ID - 50035: Ensure that Microsoft Entra authentication is configured for SQL Servers.

Control ID - 50036: Ensure that Resource Locks are set for Mission-Critical Azure Resources.

Control ID - 50039: Ensure Enforce SSL connection is set to ENABLED for MySQL Database Server.

Control ID - 50040: Ensure Enforce SSL connection is set to ENABLED for PostgreSQL Database Server.

Control ID - 50041: Ensure server parameter log_checkpoints is set to ON for PostgreSQL Database Server

Control ID - 50042: Ensure server parameter log_connections is set to ON for PostgreSQL Database Server.

Control ID - 50043: Ensure server parameter log_disconnections is set to ON for PostgreSQL Database Server.

Control ID - 50045: Ensure server parameter log_retention_days is greater than 3 days for PostgreSQL Database Server

Control ID - 50047: Ensure App Service Authentication is set up for apps in Azure App Service.

Control ID - 50048: Ensure Web app redirects all HTTP traffic to HTTPS.

Control ID - 50050: Ensure that Register with Entra ID is enabled on App Service.

Control ID - 50051: Ensure Web app is using the latest version of TLS encryption version.

Control ID - 50052: Ensure default network access rule for Storage Accounts is set to deny.

Control ID - 50053: Ensure Allow Azure services on the trusted services list to access this storage account is Enabled for Storage Account Access

Control ID - 50055: Ensure Network Security Group Flow Log retention is greater than 90 days.

Control ID - 50056: Ensure the storage account containing the container with activity logs is encrypted with Customer Managed Key

Control ID - 50059: Ensure Activity Log Alert exists for Delete SQL server firewall rule.

Control ID - 50061: Ensure that HTTP Version used for web app is latest.

Control ID - 50062: Ensure Network Watcher is Enabled for your Subscription.

Control ID - 50063: Ensure Activity Log Alert exists for Create Policy Assignment.

Control ID - 50064: Ensure Activity Log Alert exists for Create or Update Network Security Group.

Control ID - 50065: Ensure Activity Log Alert exists for Delete Network Security Group.

Control ID - 50068: Ensure Activity Log Alert exists for Create or Update Security Solution.

Control ID - 50069: Ensure Activity Log Alert exists for Delete Security Solution.

Control ID - 50070: Ensure Activity Log Alert exists for Create or Update SQL Server Firewall Rule.

Control ID - 50072: Ensure guest users are reviewed on a monthly basis.

Control ID - 50073: Ensure that no custom subscription Administrator Roles exist.

Control ID - 50074: Ensure server parameter connection_throttling is set to ON for PostgreSQL Database Server.

Control ID - 50075: Ensure that diagnostic settings for Azure KeyVault is set to ON.

Control ID - 50077: Ensure that Microsoft Defender for Cloud Apps integration with Microsoft Defender for Cloud is Selected

Control ID - 50078: Ensure that Microsoft Defender for Endpoint integration with Microsoft Defender for Cloud is selected

Control ID - 50079: Ensure that Microsoft Defender for Azure SQL Databases is set to On.

Control ID - 50080: Ensure that Microsoft Defender for App Services is set to On.

Control ID - 50081: Ensure that Microsoft Defender for Storage is set to On.

Control ID - 50099: Ensure that Azure Cosmos DB accounts Firewalls and Networks is limited to use Selected Networks instead of All Networks

Control ID - 50117: Ensure Allow access to Azure services for PostgreSQL Database Server is disabled.

Control ID - 50130: Ensure that the endpoint protection for all Virtual Machines is installed.

Control ID - 50133: Ensure Soft Delete is Enabled for Azure Containers and Blob Storage.

Control ID - 50134: Ensure Storage for Critical Data are Encrypted with Customer Managed Keys.

Control ID - 50135: Ensure Activity Log Alert exists for Delete Policy Assignment.

Control ID - 50136: Ensure FTP deployments are disabled for web apps.

Control ID - 50137: Ensure that OS and Data disks are encrypted with Customer Managed Key.

Control ID - 50138: Ensure that UDP Services are restricted from the Internet.

Control ID - 50140: [LEGACY] Ensure that Microsoft Defender is set to On for Container Registries.

Control ID - 50141: Ensure that Microsoft Defender for Key Vault is set to On.

Control ID - 50142: Ensure Diagnostic Setting captures appropriate categories.

Control ID - 50172: Ensure that Microsoft Defender for Open-Source Relational Databases is set to On.

Control ID - 50175: Ensure that Storage Accounts have infrastructure encryption enabled.

Control ID - 50176: Ensure that Azure Key Vaults use Private Links.

Control ID - 50181: Ensure Storage Accounts are using the latest version of TLS encryption.

Control ID - 50197: [LEGACY] Ensure that Microsoft Defender for DNS is set to On.

Control ID- 50215: Ensure Storage logging is enabled for Queue service for read, write and delete requests. 104

Control ID - 50218: Ensure that the expiry date is set on all keys from RBAC key Vault. 106

Control ID - 50223: Ensure that Only Approved Extensions Are Installed. 107

Control ID - 50226: Ensure that Microsoft Defender for Resource Manager is set to On. 108

Azure Database Service Best Practices Policy

Control ID - 50096: Ensure Storage Auto-Growth is enabled on PostgreSQL server.

Control ID - 50098: Ensure that ssl_minimal_tls_version_enforced is set to 1.2 for SQL server.

Control ID - 50100: Ensure that Azure SQL Database have private endpoint connections enabled.

Control ID - 50103: Ensure that ssl_minimal_tls_version_enforced is set to 1.2 for Azure Database for MySQL server

Control ID - 50104: Ensure no MySQL Server allow ingress from Internet (ANY IP)

Control ID - 50105: Ensure that geo_redundant_backup_enabled is set to Enabled for Azure Database for MySQL server

Control ID - 50106: Ensure that Public Network Access is Disabled for Azure Database for MySQL server

Control ID - 50107: Ensure that Azure Database for MySQL server diagnostic setting is configured properly.

Control ID - 50108: Ensure SQL server has Auto-Failover group enabled.

Control ID - 50109: Ensure Enforce SSL connection is set to ENABLED for Azure Database for MariaDB server.

Control ID - 50110: Ensure that ssl_minimal_tls_version_enforced is set to 1.2 for Azure Database for MariaDB server

Control ID - 50111: Ensure no MariaDB Server allow ingress from Internet (ANY IP)

Control ID - 50112: Ensure that geo_redundant_backup_enabled is set to Enabled for Azure Database for MariaDB server

Control ID - 50113: Ensure that Public Network Access is Disabled for Azure Database for MariaDB server

Control ID - 50116: Ensure that ssl_minimal_tls_version_enforced is set to 1.2 for Azure Database for PostgreSQL server

Control ID - 50118: Ensure that geo_redundant_backup_enabled is set to Enabled for Azure Database for PostgreSQL server

Control ID - 50119: Ensure that Public Network Access is Disabled for Azure Database for PostgreSQL server

Control ID - 50120: Ensure that Azure Database for PostgreSQL server diagnostic setting is configured properly.

Control ID - 50121: Ensure that Automatic-failover is set for Azure CosmosDB.

Control ID - 50122: Ensure that Diagnostic settings are set properly for Azure CosmosDB.

Control ID - 50123: Ensure that resource lock is set on Azure CosmosDB.

Control ID - 50124: Ensure that Azure CosmosDB does not allow access from all networks.

Control ID - 50131: Ensure that Azure Active Directory authentication is configured for MySql server.

Control ID - 50132: Ensure that Azure Active Directory authentication is configured for PostgreSql servers.

Control ID - 50177: Ensure that encryption with customer-managed key is enabled in PostgreSQL servers.

Control ID - 50178: Ensure that public network access is disabled on Azure SQL databases.

Control ID - 50179: Ensure that public network access is disabled for MySQL flexible servers.

Control ID - 50180: Ensure that public network access is disabled for PostgreSQL flexible servers.

Control ID - 50221: Ensure consistency level is not set to Eventual for Azure CosmosDB account

Control ID - 50240: Ensure that PostgreSQL server has infrastructure encryption enabled.

Control ID - 50243: Ensure that Cosmos DB accounts have customer-managed keys to encrypt data at rest.

Control ID - 50263: Ensure that MySQL server has infrastructure encryption enabled.

Control ID - 50268: Ensure that encryption with customer-managed key is enabled in MySQL Servers.

Control ID - 50349: Ensure missing service endpoints are disabled for Azure PostgreSQL Virtual Network Rule.

Control ID - 50350: Ensure tags are associated with Azure CosmosDB account

Azure Function App Best Practices Policy

Control ID - 50058: Ensure that Detailed Error Logging is enabled in API Apps

Control ID - 50084: Ensure App Service Authentication is set on Function Apps

Control ID - 50085: Ensure Function app redirects all HTTP traffic to HTTPS

Control ID - 50086: Ensure Function app has "Client Certificates (Incoming client certificates)" set to "On"

Control ID - 50087: Ensure that "Register with Azure Active Directory" is enabled on Function apps

Control ID - 50088: Ensure Function app is using the latest version of TLS encryption version

Control ID - 50089: Ensure that "HTTP Version" used for Function app is latest

Control ID - 50143: Ensure that CORS does not allow every resource to access the Function Apps

Control ID - 50146: Ensure that Function apps enforce FTPS-only access to FTP traffic

Control ID - 50147: Ensure that Managed identity is used in Function apps

Control ID - 50149: Ensure that Remote debugging is turned off for Function apps

Control ID - 50151: Ensure that routing of outbound non-RFC 1918 traffic to Azure Virtual Network is enabled in Function apps

Control ID - 50385: Ensure there is a sufficient backup retention period configured for Azure API App Services applications

Control ID - 50386: Ensure there is a sufficient backup retention period configured for Azure Web App Services applications

Control ID - 50387: Ensure that all your Azure API App Services applications are using the Backup and Restore feature

Control ID - 50388: Ensure that all your Azure App Services applications are using the Backup and Restore feature in Web App

Azure Best Practices Policy

Control ID - 50003: Ensure that Adaptive Application Controls is set to On

Control ID - 50006: Ensure that Vulnerabilities in security configuration on your machines should be remediated is set to On

Control ID - 50007: Ensure that Monitor missing Endpoint Protection in Azure Security Center is set to On

Control ID - 50009: Ensure that Network security groups is set to On

Control ID - 50010: Ensure that NSGs rules for web applications on IaaS should be hardened is set to ON

Control ID - 50014: Ensure that Monitor unaudited SQL databases in Azure Security Center is set to On

Control ID - 50017: Ensure that Vulnerabilities should be remediated by a Vulnerability Assessment solution

Control ID - 50018: Ensure that Audit missing blob encryption for storage account is set to On

Control ID - 50019: Ensure that Just-In-Time network access control should be applied on virtual machines is set to On

Control ID - 50021: Ensure that security contact Phone number is set

Control ID - 50024: Ensure that LogProfile for a subscription is configured properly

Control ID - 50025: Ensure that Monitor unencrypted SQL databases in Azure Security Center is set to On

Control ID - 50033: Ensure that all Attached VM Disks are encrypted with Customer Managed Key (CMK)

Control ID - 50034: Ensure disks are encrypted for Windows VMs with ADE version 1.1

Control ID - 50037: Ensure to enable Virtual machines with end-to-end encryption using encryption at host

Control ID - 50038: Ensure that all disk snapshots are encrypted with Customer-managed key(CMK)

Control ID - 50046: Enable RBAC within Azure Kubernetes Services

Control ID - 50054: Ensure that logging for Azure KeyVault is Enabled

Control ID - 50057: Ensure that Azure Container Registry not using deprecated classic registry

Control ID - 50058: Ensure that Detailed Error Logging is enabled in API Apps

Control ID - 50060: Ensure that Azure Virtual Network subnet is configured with a Network Security Group

Control ID - 50066: Ensure Activity Log Alert exists for Create or Update Network Security Group Rule

Control ID - 50067: Ensure Activity Log Alert exists for Delete Network Security Group Rule

Control ID - 50071: Ensure Activity Log Alert exists for Update Security Policy

Control ID - 50090: Ensure that Azure AKS cluster monitoring is enabled

Control ID - 50091: Ensure that Azure AKS cluster HTTP application routing is disabled

Control ID - 50092: Ensure that Azure AKS cluster Azure CNI networking enabled

Control ID - 50093: Ensure that Azure Application Gateway have the Web application firewall (WAF) enabled

Control ID - 50094: Ensure that Azure Application Gateway allows TLSv1.2 or above

Control ID - 50097: Ensure that Request Tracing is enabled in API Apps

Control ID - 50101: Ensure that Logic Apps Integration Service Environments are encrypted with customer-managed keys

Control ID - 50114: Ensure that network access is restricted in Cognitive Services accounts

Control ID - 50125: Ensure Activity Log Alert exists for Create/Update Storage Account

Control ID - 50126: Ensure Activity Log Alert exists for Delete Storage Account

Control ID - 50127: Ensure Activity Log Alert exists for Create or Update Virtual Machine

Control ID - 50128: Ensure Activity Log Alert exists for Deallocate Virtual Machine

Control ID - 50129: Ensure Activity Log Alert exists for Delete Virtual Machine

Control ID - 50139: Ensure that Azure Defender is set to On for Kubernetes

Control ID - 50144: Ensure that CORS does not allow every resource to access the Web apps

Control ID - 50145: Ensure that Diagnostic logs is enabled in Web apps

Control ID - 50148: Ensure that Managed identity is used in Web apps

Control ID - 50150: Ensure that Remote debugging is turned off for Web apps

Control ID - 50152: Ensure that outbound non-RFC 1918 traffic to Azure Virtual Network is enabled in Web apps

Control ID - 50153: Ensure that public network access is disabled in Redis Cache

Control ID - 50154: Ensure that Redis Cache uses private link

Control ID - 50155: Ensure that only secure connections to Redis Cache is enabled

Control ID - 50156: Ensure that public network access is disabled in Managed Disks

Control ID - 50157: Ensure that Disk Access resources are configured with private endpoints

Control ID - 50158: Ensure that all Authorization Rules except RootManageSharedAccessKey are removed from Event Hub Namespaces

Control ID - 50159: Ensure that Authorization rules are defined in Event Hub instances

Control ID - 50160: Ensure that Event Hub Namespaces use Customer-Managed Key for encryption

Control ID - 50161: Ensure that Event Hub Namespaces use private links

Control ID - 50162: Ensure that Resource Logs are enabled in Event Hub Namespaces

Control ID - 50163: Ensure that all Authorization Rules except RootManageSharedAccessKey are removed from Service Bus Namespaces

Control ID - 50164: Ensure that Service Bus Namespaces use private links

Control ID - 50165: Ensure that Resource Logs are enabled in Service Bus Namespaces

Control ID - 50166: Ensure that Azure Linux-based virtual machines (VMs) are configured to use SSH keys

Control ID - 50167: Ensure that Azure Container Instance container groups use customer-managed key for encryption

Control ID - 50168: Ensure that Advanced Threat Protection is enabled for all Microsoft Azure Cosmos DB accounts

Control ID - 50169: Ensure that Advanced Threat Protection is enabled on Storage Accounts

Control ID - 50170: Ensure that Azure File Sync uses private link

Control ID - 50171: Ensure that Azure Redis Cache servers are using the latest version of the TLS protocol

Control ID - 50173: Ensure that Geo-redundant storage is enabled for Storage Accounts

Control ID - 50174: Ensure that Public network access is disabled for Azure File Sync

Control ID - 50182: Ensure that monitoring of DDoS protection at the Azure virtual network level is enabled

Control ID - 50183: Ensure that monitoring of deprecated accounts within your Azure subscription(s) is enabled

Control ID - 50184: Ensure that IP forwarding enablement on your Azure virtual machines (VMs) is being monitored

Control ID - 50185: Ensure that the external accounts with write permissions are monitored using Azure Security Center

Control ID - 50186: Ensure that critical Azure Blob Storage data is protected from accidental deletion or modification

Control ID - 50187: Ensure that Diagnostic Settings for Storage Accounts are configured with Log Analytics workspace

Control ID - 50188: Ensure that Diagnostic Settings for Storage Blobs are configured with Log Analytics workspace

Control ID - 50189: Ensure that Diagnostic Settings for Storage Files are configured with Log Analytics workspace

Control ID - 50190: Ensure that Diagnostic Settings for Storage Queues are configured with Log Analytics workspace

Control ID - 50191: Ensure that Diagnostic Settings for Storage Tables are configured with Log Analytics workspace

Control ID - 50192: Ensure that Azure Kubernetes Service Private Clusters is enabled

Control ID - 50193: Ensure that Azure Policy Add-on for Kubernetes service (AKS) is installed and enabled on your clusters

Control ID - 50194: Ensure that Azure Event Grid topics use private links

Control ID - 50195: Ensure that Azure Cache for Redis resides within virtual network

Control ID - 50196: Ensure that Diagnostic logs are enabled in Virtual Machine Scale Sets

Control ID - 50198: Ensure that Storage Accounts use private link connections

Control ID - 50199: Ensure that Container Registries are configured to disable public network access

Control ID - 50200: Ensure that Container Registries are configured with private endpoints

Control ID - 50201: Ensure that Container Registries are encrypted with a customer-managed key

Control ID - 50202: Ensure that FTPS is enforced in API Apps

Control ID - 50203: Ensure that Managed Identity is used in API Apps

Control ID - 50204: Ensure that API Apps are only accessible over HTTPS

Control ID - 50205: Ensure that API Apps have Incoming Client Certificates is set to On

Control ID - 50206: Ensure that HTTP Logging is enabled in API Apps

Control ID - 50208: Ensure that Kubernetes Services Management API server is configured with restricted access

Control ID - 50210: Ensure that Kube Dashboard is disabled

Control ID - 50217: Ensure that audit profile captures all the activities

Control ID - 50224: Ensure that managed virtual network is enabled in Azure Synapse workspaces

Control ID - 50225: Ensure that Storage accounts disallow Blob public access

Control ID - 50227: Ensure that Automation account variables are encrypted

Control ID - 50228: Ensure that Azure Data Explorer uses disk encryption

Control ID - 50229: Ensure that Azure Data Explorer uses double encryption

Control ID - 50230: Ensure that Azure Batch account uses key vault to encrypt data

Control ID - 50236: Ensure that Web Apps use Azure Files

Control ID - 50239: Ensure that automatic OS image patching is enabled for Virtual Machine Scale Sets

Control ID - 50241: Ensure that Virtual Machine Scale Sets have encryption at host enabled

Control ID - 50242: Ensure that Azure Container Instance container groups are deployed in a virtual network

Control ID - 50244: Ensure that Azure Data Factory uses Git repository for source control

Control ID - 50245: Ensure that public network access is disabled in Azure Data Factory

Control ID - 50246: Ensure that encryption is enabled for Data Lake Store accounts

Control ID - 50248: Ensure that API Management services use virtual networks

Control ID - 50249: Ensure that public network access is disabled for Azure IoT Hub

Control ID - 50250: Ensure that Firewall is enabled on Key Vaults

Control ID - 50251: Ensure that Key Vault keys are backed by HSM

Control ID - 50252: Ensure that Azure Event Grid domains should have local authentication methods disabled

Control ID - 50253: Ensure that Key Vault Secrets have Content-Type set

Control ID - 50254: Ensure that Azure Kubernetes Service uses disk encryption set

Control ID - 50255: Ensure that IP forwarding is disabled for Network Interfaces

Control ID - 50257: Ensure that Web Application Firewall (WAF) is enabled in Azure Front Door Services

Control ID - 50260: Ensure that public network access is disabled for Cognitive Services accounts

Control ID - 50261: Ensure that Service Fabric cluster has the ClusterProtectionLevel property set to EncryptAndSign

Control ID - 50262: Ensure that Service Fabric cluster uses Azure Active Directory for authentication

Control ID - 50265: Ensure that encryption at rest uses customer-managed key in Azure Data Explorer

Control ID - 50267: Ensure that Azure Data Factory is encrypted with a customer-managed key

Control ID - 50273: Ensure that Azure Event Grid topics should have local authentication methods disabled

Control ID - 50274: Ensure that Diagnostic logs are enabled in Data Lake Analytics accounts

Control ID - 50275: Ensure that Diagnostic logs are enabled in Azure Data Lake Storage accounts

Control ID - 50276: Ensure that Diagnostic logs are enabled in Search Services

Control ID - 50277: Ensure that Diagnostic logs are enabled in Logic Apps

Control ID - 50278: Ensure that Container Registry disallows unrestricted network access

Control ID - 50279: Ensure that Azure Kubernetes Service (AKS) cluster has Network Policy configured

Control ID - 50280: Ensure that public network access is disabled for IoT Hub Device Provisioning Service instances

Control ID - 50281: Ensure that IoT Hub Device Provisioning Service instances use private links

Control ID - 50282: Ensure that Resource logs are enabled in IoT Hub

Control ID - 50283: Ensure that Azure Data Factory Integration Runtimes have a limit for the number of cores

Control ID - 50284: Ensure that Azure Data Factory uses private link

Control ID - 50285: Ensure that SQL Server Integration Services Integration Runtimes on Azure Data Factory are joined to a virtual network

Control ID - 50286: Ensure that Virtual network injection is enabled for Azure Data Explorer

Control ID - 50287: Ensure that public network access is disabled for Automation accounts

Control ID - 50288: Ensure that Automation account uses customer-managed keys to encrypt data at rest

Control ID - 50289: Ensure that Automation account has private endpoint connections enabled

Control ID - 50290: Ensure that Azure Batch pools have disk encryption enabled

Control ID - 50291: Ensure that Azure Batch accounts have local authentication methods disabled

Control ID - 50292: Ensure that Metric alert rules are configured on Batch accounts

Control ID - 50293: Ensure that Batch accounts have private endpoint connections enabled

Control ID - 50294: Ensure that public network access is disabled for Batch accounts

Control ID - 50295: Ensure that Resource logs are enabled in Batch accounts

Control ID - 50296: Ensure that Cognitive Services enable data encryption with customer-managed keys

Control ID - 50297: Ensure that Cognitive Services have local authentication methods disabled

Control ID - 50298: Ensure that Managed identity is used in Cognitive Services

Control ID - 50299: Ensure that Cognitive Services use private links

Control ID - 50300: Ensure that Azure Event Grid domains are configured to disable public network access

Control ID - 50301: Ensure that public network access is disabled in Azure Event Grid topics

Control ID - 50302: Ensure that Azure Event Grid domains use private links

Control ID - 50303: Ensure that API Management Services use latest protocol for Client Side Security

Control ID - 50304: Ensure that API Management Services use latest protocol for Backend Side Transport Security

Control ID - 50305: Ensure that API Management services use a SKU that supports virtual networks

Control ID - 50306: Ensure that Cipher Triple DES (3DES) is enabled for API Management resource

Control ID - 50307: Ensure that HTTP/2 client side protocol is enabled for API Management resource

Control ID - 50308: Ensure that System assigned Managed Identity is enabled for API Management Service

Control ID - 50309: Ensure that Logic Apps are deployed into Integration Service Environment

Control ID – 50321: Ensure that Azure Event Grid partner namespaces should have local authentication methods disabled

Control ID – 50323: Ensure that Azure Event Hub namespaces should have local authentication methods disabled

Control ID - 50324: Ensure that Front Door WAF prevents message lookup in Log4j2

Control ID - 50325: Ensure that Application Gateway WAF prevents message lookup in Log4j2

Control ID - 50328: Ensure that Application Insights retention Period is 90 days or more

Control ID - 50329: Ensure that Application Insights components block log ingestion and querying from public networks

Control ID - 50330: Ensure that protocol used by CDN profile endpoints is HTTPS

Control ID - 50331: Ensure azure spring cloud service apps have end to end TLS enabled

Control ID - 50332: Ensure that azure spring cloud service apps have HTTPS enabled

Control ID - 50333: Ensure that Application Insights are enabled for azure spring cloud service

Control ID - 50334: Ensure that Diagnostic settings is enabled for azure spring cloud resource service

Control ID - 50337: Ensure access to Azure SQL Servers is restricted within Azure Infrastructure via Azure SQL Firewall Rule

Control ID - 50338: Ensure public accessibility is not enabled for Azure MSSQL Server

Control ID - 50339: Ensure that App Services web applications have always-on feature enabled

Control ID - 50340: Ensure zone resiliency is turned on for Azure Image

Control ID - 50341: Ensure web sockets are disabled for Azure App Service

Control ID - 50342: Ensure read-only cache is enabled on OS disks with read heavy operations to get higher read IOPS for Azure Image

Control ID - 50344: Ensure that IP restriction rules are configured for Azure App Service

Control ID - 50345: Ensure data exfiltration protection is enabled for Azure Synapse Workspace

Control ID - 50346: Ensure Hyper-V generation uses v2 for Azure Image

Control ID - 50347: Ensure firewall rules reject internet access for Azure Redis Cache

Control ID - 50348: Ensure that public network access is disabled for Azure Synapse Workspace

Control ID - 50351: Ensure age in days after create to delete snapshot is more than 90 in Azure Storage Management Policy

Control ID - 50352: Ensure overprovisioning is disabled for Azure Linux Virtual Machine Scale Set

Control ID – 50353: Ensure that Azure Event Hub namespaces should have double encryption enabled

Control ID - 50354: Ensure user ids are system managed for Azure Container Group

Control ID - 50355: Ensure that VPN Encryption is enabled for Azure Virtual WAN

Control ID - 50356: Ensure use of NSG with Azure Virtual Machine Scale Set

Control ID - 50357: Ensure flow logging is enabled for Azure Network Watcher via Azure Network Watcher Flow Log

Control ID - 50358: Ensure that admin user is disabled for Azure Container Registry

Control ID - 50359: Ensure queries over the public internet are not supported for Azure Log Analytics Workspace

Control ID - 50361: Ensure overprovisioning is disabled for Azure Windows Virtual Machine Scale Set

Control ID - 50362: Ensure log analytics workspace has daily quota value set for Azure Log Analytics Workspace

Control ID - 50364: Ensure that Azure HDInsight clusters should be injected into a virtual network

Control ID - 50365: Ensure end-to-end TLS is enabled to encrypt and securely transmit sensitive data to the backend for Azure Application Gateway

Control ID - 50366: Ensure HTTP is disallowed for Azure CDN Endpoint

Control ID - 50367: Ensure auto inflate is enabled for Azure Eventhub Namespace

Control ID - 50368: Ensure data backup is enabled using blob container uri for Azure Analysis Services Servers

Control ID - 50369: Ensure compression is enabled for Azure CDN Endpoint

Control ID - 50370: Ensure Power BI analysis services are defined for Azure Analysis Services Server

Control ID – 50371: Ensure that Azure HDInsight clusters should use customer-managed keys to encrypt data at rest

Control ID - 50372: Ensure that a resource locking administrator role is available for each Azure subscription.

Control ID - 50373: Ensure that an activity log alert is created for Create or Update Load Balancer events

Control ID - 50374: Ensure that an activity log alert is created for Create or Update Azure SQL Database events

Control ID - 50375: Ensure that an activity log alert is created for Delete Azure SQL Database events

Control ID - 50376: Ensure there is an activity log alert created for the Delete Key Vault events

Control ID - 50377: Ensure there is an Azure activity log alert created for Delete Load Balancer events

Control ID - 50378: Ensure that an activity log alert exists for Power Off Virtual Machine events

Control ID - 50379: Ensure that an activity log alert is created for Rename Azure SQL Database events

Control ID - 50380: Ensure that an activity log alert is created for Update Key Vault (Microsoft.KeyVault/vaults) events

Control ID - 50381: Ensure that an activity log alert is created for Create/Update MySQL Database events

Control ID - 50382: Ensure that an activity log alert is created for Create/Update PostgreSQL Database events

Control ID - 50383: Ensure that an activity log alert is created for Delete MySQL Database events

Control ID - 50384: Ensure that an activity log alert is created for Delete PostgreSQL Database events

Control ID - 50389: Ensure that Azure virtual machine scale sets are configured for zone redundancy

Control ID - 50390: Ensure that Azure Log Profile is configured to export all control and management activities

Control ID - 50391: Ensure that Azure Search Service instances are configured to use system-assigned managed identities

Control ID - 50392: Ensure that Azure Blob Storage service has a lifecycle management policy configured

Control ID- 50393: Ensure that Azure Storage account access is limited only to specific IP address(es)

Control ID - 50394: Ensure there are budget alerts configured to warn about forthcoming budget overages within your Azure cloud account

Control ID – 50395: Ensure that Azure HDInsight clusters should use encryption at host to encrypt data at rest

Control ID – 50396: Ensure that Azure HDInsight clusters should use encryption in transit to encrypt communication between Azure HDInsight cluster nodes

Control ID – 50397: Enusre that Azure HDInsight clusters are configured with private endpoints

Control ID – 50398: Ensure that CORS does not allow every domain to access your FHIR Service

Control ID - 50457: Ensure that Linux and Windows Disk encryption should be applied on virtual machines is set to On

Control ID - 50458: Ensure that 'cross-tenant replication' is set to disabled

Control ID – 50459: Ensure that Azure Application Gateway have Web application firewall (WAF) V2 enabled which has policy attached

Control ID - 52000: Ensure that corporate login credentials are used instead of Gmail accounts

Control ID - 52001: Ensure that there are only GCP-managed service account keys for each service account

Control ID - 52002: Ensure that no Project has ServiceAccount with Admin privileges

Control ID - 52003: Ensure that IAM users are not assigned Service Account User role at project level

Control ID - 52004: Ensure user-managed/external keys for service accounts are rotated every 90 days or less

Control ID - 52005: Ensure KMS encryption keys are rotated within a period of 90 days

Control ID - 52006: Ensure that Separation of duties is enforced while assigning KMS related roles

Control ID - 52007: Ensure that IAM users are not assigned Service Account Token Creator role at project level

Control ID - 52008: Ensure that Cloud Audit Logging is configured properly across all services and all users from a project

Control ID - 52009: Ensure that sinks are configured for all log entries

Control ID - 52011: Ensure log metric filter and alerts exists for Project Ownership assignments/changes

Control ID - 52012: Ensure log metric filter and alerts exists for Audit Configuration Changes

Control ID - 52013: Ensure log metric filter and alerts exists for Custom Role changes

Control ID - 52014: Ensure log metric filter and alerts exists for VPC Network Firewall rule changes

Control ID - 52015: Ensure log metric filter and alerts exists for VPC network route changes

Control ID - 52016: Ensure log metric filter and alerts exists for VPC network changes

Control ID - 52017: Ensure log metric filter and alerts exists for Cloud Storage IAM permission changes

Control ID - 52018: Ensure log metric filter and alerts exists for SQL instance configuration changes

Control ID - 52019: Ensure the default network does not exist in a project

Control ID - 52020: Ensure that IP forwarding is not enabled on Instances

Control ID - 52021: Ensure that SSH access is restricted from the internet

Control ID - 52022: Ensure that RDP access is restricted from the internet

Control ID - 52024: Ensure VPC Flow logs is enabled for every subnet in VPC Network

Control ID - 52025: Ensure that instances are not configured to use the default service account with full access to all Cloud APIs

Control ID - 52026: Ensure Block Project-wide SSH keys enabled for VM instances

Control ID - 52027: Ensure oslogin is enabled for a Project

Control ID - 52028: Ensure connecting to serial ports is not enabled for VM Instance

Control ID - 52029: Ensure VM disks for critical VMs are encrypted with Customer-Supplied Encryption Keys (CSEK)

Control ID - 52030: Ensure that Cloud Storage bucket is not anonymously or publicly accessible

Control ID - 52032: Ensure that Cloud SQL - Mysql database instance requires all incoming connections to use SSL

Control ID - 52033: Ensure that Cloud SQL - Mysql database Instances are not open to the world

Control ID - 52034: Ensure legacy networks do not exist for a project

Control ID - 52035: Ensure that MySQL Database Instance does not allows root login from any Host

Control ID - 52036: Ensure that Cloud Storage buckets have uniform bucket-level access enabled

Control ID - 52059: Ensure log_connections database flag for Cloud SQL - PostgreSQL instance is set to on

Control ID - 52060: Ensure log_disconnections database flag for Cloud SQL - PostgreSQL instance is set to on

Control ID - 52062: Ensure log_error_verbosity database flag for Cloud SQL - PostgreSQL instance is set to DEFAULT or stricter

Control ID - 52063: Ensure log_statement database flag for Cloud SQL - PostgreSQL instance is set to ddl or stricter

Control ID - 52064: Ensure log_hostname database flag for Cloud SQL - PostgreSQL instance is set to off

Control ID - 52065: Ensure that Cloud SQL - PostgreSQL database instance requires all incoming connections to use SSL

Control ID - 52066: Ensure that Cloud SQL - PostgreSQL database Instances are not open to the world

Control ID - 52067: Ensure that Cloud SQL - SQL Server database instance requires all incoming connections to use SSL

Control ID - 52068: Ensure that Cloud SQL - SQL Server database Instances are not open to the world

Control ID - 52071: Ensure log_min_error_statement database flag for Cloud SQL - PostgreSQL instance is set to Error or stricter

Control ID - 52072: Ensure log_min_messages database flag for Cloud SQL - PostgreSQL instance is set to Error or stricter

Control ID - 52073: Ensure log_min_duration_statement database flag for Cloud SQL - PostgreSQL instance is set to -1(disabled)

Control ID - 52075: Ensure skip_show_database database flag for Cloud SQL - Mysql instance is set to on

Control ID - 52076: Ensure local_infile database flag for Cloud SQL - Mysql instance is set to off

Control ID - 52077: Ensure external scripts enabled database flag for Cloud SQL - SQL Server instance is set to off

Control ID - 52078: Ensure cross db ownership chaining database flag for Cloud SQL - SQL Server instance is set to off

Control ID - 52080: Ensure user options database flag for Cloud SQL - SQL Server instance is not configured

Control ID - 52081: Ensure access database flag for Cloud SQL - SQL Server instance is set to off

Control ID - 52082: Ensure 3625 (trace flag) database flag for Cloud SQL - SQL Server instance is set to off

Control ID - 52083: Ensure contained database authentication database flag for Cloud SQL - SQL Server instance is set to off

Control ID - 52084: Ensure Cloud SQL - MySql Instance do not have public IP addresses

Control ID - 52085: Ensure Cloud SQL - SQL server Instance do not have public IP addresses

Control ID - 52086: Ensure Cloud SQL - PostgreSQL Instance do not have public IP addresses

Control ID - 52087: Ensure Cloud SQL - MySql instance is configured with automated backups

Control ID - 52088: Ensure Cloud SQL - SQL server is configured with automated backups

Control ID - 52089: Ensure Cloud SQL - PostgreSQL instance is configured with automated backups

Control ID - 52090: Ensure that Cloud KMS cryptokeys are not anonymously or publicly accessible

Control ID - 52091: Ensure Compute instances are launched with Shielded VM enabled

Control ID - 52093: Ensure that instances are not configured to use default service account

Control ID - 52094: Ensure that Compute instances do not have public IP addresses

Control ID - 52095: Ensure that BigQuery Dataset is encrypted with Customer-managed key

Control ID - 52096: Ensure that BigQuery Table is encrypted with Customer-managed key

Control ID - 52098: Ensure that BigQuery datasets are not anonymously or publicly accessible

Control ID - 52099: Ensure that retention policies on Log Buckets are configured using bucket lock

Control ID - 52100: Ensure that DNSSEC is enabled for Cloud DNS

Control ID - 52109: Ensure that GCP Cloud DNS zones is not using RSASHA1 algorithm for DNSSEC key-signing

Control ID - 52110: Ensure that GCP Cloud DNS zones is not using RSASHA1 algorithm for DNSSEC zone-signing

Control ID - 52111: Ensure that Compute instances have Confidential Computing enabled

Control ID - 52116: Ensure that Cloud DNS logging is enabled for all VPC networks

Control ID - 52132: Ensure there are no API keys associated with your Google Cloud Platform (GCP) project

Control ID - 52148: Ensure user connections database flag for Cloud SQL - SQL Server instance is set to appropriate value

Control ID - 52161: Ensure that your Dataproc clusters are encrypted using Customer-Managed Keys (CMKs)

Control ID - 52172: Ensure that API keys are restricted to only those APIs that application needs access to

Control ID - 52173: Ensure there are no unrestricted API keys available within your Google Cloud Platform (GCP) project

Control ID - 52174: Ensure that logging is enabled for Google Cloud global load balancing backend services

Control ID - 52175: Ensure Cloud Asset Inventory Is Enabled

Control ID - 52176: Ensure that cloudsql.enable_pgaudit database flag for each Cloud Sql Postgresql Instance is set to on for Centralized Logging

Control ID - 52177: Ensure API Keys are rotated every 90 days

Control ID - 52178: Ensure Cloud SQL - PostgreSQL Instance IP assignment is set to private

Control ID – 52179: Ensure That Separation of Duties Is Enforced While Assigning Service Account Related Roles to Users

GCP Best Practices Policy

Control ID - 52010: Ensure that object versioning is enabled on buckets

Control ID - 52023: Ensure Private Google Access is enabled for all subnetwork in VPC Network

Control ID - 52031: Ensure that logging is enabled for Cloud storage buckets

Control ID - 52057: Ensure that there are no harmful object life cycle rules are created on Storage Buckets

Control ID - 52058: Ensure that object retention policy is set on storage buckets

Control ID - 52092: Ensure "oslogin" is enabled for VM instance

Control ID - 52108: Ensure that GCP Storage bucket is encrypted using customer-managed key

Control ID - 52118: Ensure that Pub/Sub topics are encrypted using Customer-Managed Keys (CMKs)

Control ID - 52120: Ensure that On Host Maintenance configuration setting is set to Migrate for all VM instances

Control ID - 52135: Ensure Default Service account is not used at a project level

Control ID - 52138: Ensure no roles that enable to impersonate and manage all service accounts are used at a project level

Control ID - 52140: Ensure that Bucket should not log to itself

Control ID - 52156: Ensure that Google Cloud Storage objects are using a lifecycle configuration for cost management

Control ID - 52157: Ensure that the Auto-Delete feature is disabled for the disks attached to your VM instances

Control ID - 52158: Ensure that your production Google Cloud virtual machine instances are not preemptible

Control ID - 52159: Ensure that deletion protection is enabled for your Google Cloud virtual machine (VM) instances

Control ID - 52160: Ensure that your virtual machine (VM) instance disks are encrypted using Customer-Managed Keys (CMKs)

Control ID - 52162: Ensure that automatic restart is enabled for VM instances

Control ID - 52168: Ensure that Cloud Armor prevents message lookup in Log4j2

Control ID - 52170: Ensure there is a dead-letter topic configured for each Pub/Sub subscription

Control ID - 52171: Ensure that your Google Cloud instance groups are using autohealing to proactively replace failing instances

GCP Cloud SQL Best Practices Policy

Control ID - 52061: Ensure "log_duration" database flag for Cloud SQL - PostgreSQL instance is set to "on"

Control ID - 52069: Ensure "log_lock_waits" database flag for Cloud SQL - PostgreSQL instance is set to "on"

Control ID - 52070: Ensure "log_temp_files" database flag for Cloud SQL - PostgreSQL instance is set to "0" (on)

Control ID - 52074: Ensure "log_checkpoints" database flag for Cloud SQL - PostgreSQL instance is set to "on"

Control ID - 52097: Ensure "default trace enabled" database flag for Cloud SQL - SQL Server instance is set to "on"

Control ID - 52106: Ensure that Cloud SQL - Mysql database instance Binary logs configuration is enabled

Control ID - 52107: Ensure that Cloud SQL - PostgreSQL database instance Point-in-time recovery is enabled

Control ID - 52112: Ensure "log_parser_stats" database flag for Cloud SQL - PostgreSQL instance is set to "off"

Control ID - 52113: Ensure "log_planner_stats" database flag for Cloud SQL - PostgreSQL instance is set to "off"

Control ID - 52114: Ensure "log_executor_stats" database flag for Cloud SQL - PostgreSQL instance is set to "off"

Control ID - 52115: Ensure "log_statement_stats" database flag for Cloud SQL - PostgreSQL instance is set to "off"

Control ID - 52119: Ensure that MySQL database instances have the slow_query_log flag set to On

Control ID - 52121: Ensure that production MySQL database instances are configured to automatically fail over to another zone within the selected cloud region

Control ID - 52122: Ensure that MySQL database servers are using the latest major version of MySQL database

Control ID - 52128: Ensure that PostgreSQL database instances have the appropriate configuration set for the max_connections flag.

Control ID - 52146: Ensure that MySQL instances are encrypted with Customer-Managed Keys (CMKs)

Control ID - 52149: Ensure that Cloud SQL PostgreSQL instance certificates are rotated (renewed) before their expiration

Control ID - 52150: Ensure that Cloud SQL MySQL instance certificates are rotated (renewed) before their expiration

Control ID - 52151: Ensure that Cloud SQL SQL Server instance certificates are rotated (renewed) before their expiration

Control ID - 52152: Ensure that production PostgreSQL database instances are configured to automatically fail over to another zone within the selected cloud region

Control ID - 52153: Ensure that production SQL Server database instances are configured to automatically fail over to another zone within the selected cloud region

Control ID - 52154: Ensure that PostgreSQL instances are encrypted with Customer-Managed Keys (CMKs)

Control ID - 52155: Ensure that SQL Server instances are encrypted with Customer-Managed Keys (CMKs)

Control ID - 52169: Ensure that automatic storage increase is enabled for your Cloud SQL database instances

GCP Kubernetes Engine Best Practices Policy

Control ID - 52037: Ensure that GCP Kubernetes cluster intra-node visibility is enabled

Control ID - 52038: Ensure Legacy Authorization is set to Disabled on Kubernetes Engine Clusters

Control ID - 52039: Ensure Kubernetes web UI / Dashboard is disabled

Control ID - 52040: Ensure Automatic node repair is enabled for Kubernetes Clusters

Control ID - 52041: Ensure Automatic node upgrades is enabled on Kubernetes Engine Clusters nodes

Control ID - 52042: Ensure that GCP Kubernetes Engine Clusters have HTTP load balancing enabled

Control ID - 52043: Ensure Network policy is enabled on Kubernetes Engine Clusters

Control ID - 52044: Ensure that GCP Kubernetes Engine Clusters have Alpha cluster feature disabled

Control ID - 52045: Ensure Kubernetes Cluster is created with Alias IP ranges enabled

Control ID - 52046: Ensure PodSecurityPolicy controller is enabled on the Kubernetes Engine Clusters

Control ID - 52047: Ensure Kubernetes Cluster is created with Private cluster enabled

Control ID - 52048: Ensure Private Google Access is set on Kubernetes Engine Cluster Subnets

Control ID - 52049: Ensure default Service account is not used for Project access in Kubernetes Clusters

Control ID - 52050: Ensure Kubernetes Clusters created with limited service account Access scopes for Project access

Control ID - 52051: Ensure Stackdriver Kubernetes Engine Monitoring is set to Enabled on Kubernetes Engine Clusters

Control ID - 52052: Ensure that Application-Layer secret encryption is enabled for Kubernetes cluster

Control ID - 52053: Ensure that Master authorized network is enabled for Kubernetes cluster

Control ID - 52079: Ensure that Google Kubernetes Engine (GKE) clusters have workload identity enabled

Control ID - 52101: Ensure Binary Authorization is set to Enabled on Kubernetes Engine Clusters

Control ID - 52102: Ensure Container-Optimized OS (cos) is used for Kubernetes Engine Clusters Node image

Control ID - 52103: Ensure GCP Kubernetes Engine Clusters are not using the default network

Control ID - 52104: Ensure that network traffic egress metering is enabled on Kubernetes Engine Clusters

Control ID - 52105: Ensure that legacy compute engine metadata endpoint for GCP Kubernetes Engine Cluster Node is disabled

Control ID - 52117: Ensure that data at rest available on your GKE clusters is encrypted with Customer-Managed Keys

Control ID - 52127: Ensure Kubernetes Clusters are configured with Labels

Control ID - 52129: Ensure that your GKE clusters nodes are shielded to protect against impersonation attacks.

Control ID - 52130: Ensure that Integrity Monitoring is enabled for your Google Kubernetes Engine (GKE) cluster nodes

Control ID - 52131: Ensure that Google Kubernetes Engine (GKE) clusters have sandbox enabled

Control ID - 52142: Ensure that the Secure Boot feature is enabled for your Google Kubernetes Engine (GKE) cluster nodes.

Control ID - 52143: Ensure the GKE Metadata Server is Enabled

Control ID - 52144: Ensure the GKE Release Channel is set

Control ID - 52147: Ensure Image Vulnerability Scanning using GCR Container Analysis or a third-party provider

GCP Cloud Functions Best Practices Policy

Control ID - 52054: Ensure that Default service account is not used for the cloud function

Control ID - 52055: Ensure that Runtime used in cloud function is not deprecated or decommissioned

Control ID - 52056: Ensure that Cloud function is not anonymously or publicly accessible

CIS Oracle Cloud Infrastructure Foundation Benchmark Policy v2.0.0

Control ID - 40001: Ensure Secure Boot is enabled on Compute Instance.

Control ID - 40002: Ensure Compute Instance boot volume has in-transit data encryption is Enabled.

Control ID - 40003: Ensure no Object Storage buckets are publicly visible.

Control ID - 40004: Ensure Versioning is Enabled for Object Storage Buckets.

Control ID - 40008: Ensure Object Storage Buckets are encrypted with a Customer Managed Key CMK.

Control ID - 40014: Ensure no security lists allow ingress from 0.0.0.0/0 or ::/0 to port 22.

Control ID - 40015: Ensure no security lists allow ingress from 0.0.0.0/0 or ::/0 to port 3389.

Control ID - 40016: Ensure the default security list of every VCN restricts all traffic except ICMP.

Control ID - 40017: Ensure MFA is enabled for all users with a console password.

Control ID - 40018: Ensure user API keys rotate within 90 days or less.

Control ID - 40019: Ensure user Customer Secret keys rotate within 90 days or less.

Control ID - 40020: Ensure user Auth Tokens rotate within 90 days or less.

Control ID - 40021: Ensure no network security groups allow ingress from 0.0.0.0/0 or ::/0 to port 22.

Control ID - 40022: Ensure no network security groups allow ingress from 0.0.0.0/0 or ::/0 to port 3389.

Control ID - 40023: Ensure API keys are not created for tenancy administrator users.

Control ID - 40024: Ensure permissions on all resources are given only to the tenancy administrator group.

Control ID - 40025: Ensure IAM administrators cannot update tenancy Administrators group.

Control ID - 40026: Ensure IAM password policy requires minimum length of 14 or greater

Control ID - 40027: Ensure default tags are used on resources.

Control ID - 40029: Ensure a Event Rule is configured for Identity Provider changes.

Control ID - 40030: Ensure a Event Rule is configured for IdP group mapping changes.

Control ID - 40031: Ensure a Event Rule is configured for IAM group changes.

Control ID - 40032: Ensure a Event Rule is configured for IAM policy changes.

Control ID - 40033: Ensure a Event Rule is configured for user changes.

Control ID - 40034: Ensure a Event Rule is configured for VCN changes.

Control ID - 40035: Ensure a Event Rule is configured for changes to route tables.

Control ID - 40036: Ensure a Event Rule is configured for security list changes.

Control ID - 40037: Ensure a Event Rule is configured for network security group changes.

Control ID - 40038: Ensure a Event Rule is configured for changes to network gateways.

Control ID - 40040: Ensure Cloud Guard is enabled in the root compartment of the tenancy.

Control ID - 40041: Ensure a Event Rule is configured for Oracle Cloud Guard problems detected.

Control ID - 40042: Ensure customer created Customer Managed Key (CMK) is rotated at least annually.

Control ID - 40044: Ensure Block Volumes are encrypted with Customer Managed Keys (CMK)

Control ID - 40045: Ensure boot volumes are encrypted with Customer Managed Key (CMK)

Control ID - 40046: Ensure File Storage Systems are encrypted with Customer Managed Keys (CMK)

Control ID - 40047: Ensure at least one compartment exists in your tenancy to store cloud resources.

Control ID - 40049: Ensure Compute Instance Legacy Metadata service endpoint is disabled.

OCI Best Practices Policy

Control ID - 40001: Ensure Secure Boot is enabled on Compute Instance

Control ID - 40002: Ensure Compute Instance boot volume has in-transit data encryption is Enabled

Control ID - 40005: Ensure Emit Object Events is Enabled for Object Storage Buckets

Control ID - 40006: Ensure Bucket Pre-Authenticated Request allows Read Only Access

Control ID - 40007: Ensure Bucket does not persists Expired Pre-Authenticated Request

Control ID - 40009: Ensure no Object Storage buckets are left Untagged

Control ID - 40010: Ensures password policy requires at least one lowercase letter

Control ID - 40011: Ensures password policy requires at least one uppercase letter

Control ID - 40012: Ensures password policy requires at least one numeric

Control ID - 40013: Ensures password policy requires at least one Special Character