Provided by:

# AWSight

*AWS Security Insights*

**awsight.com**

Comprehensive AWS security monitoring and compliance solutions designed specifically for growing businesses. Get enterprise-grade security insights without the enterprise complexity.

# AWS Security Compliance Checklist

## Complete Controls Guide for Enterprise Security

A comprehensive security checklist covering all AWS Foundational Security Best Practices, including ACM, DMS, EC2, ECS, ECR, EFS, EKS, ELB, ES, EMR, IAM, KMS, MSK, MQ, PCA, RDS, S3, SES, SNS, SQS, SSM, and WAF controls mapped to compliance frameworks.

**300+**
Security Controls

**20+**
AWS Services

**5**
Compliance Frameworks

## Why This Comprehensive Checklist Matters

AWS environments have grown exponentially in complexity, with over 200 services and thousands of configuration options. This comprehensive checklist addresses **all AWS Foundational Security Best Practices** to ensure complete coverage of your security posture.

Each control in this checklist is mapped to specific compliance frameworks including:

- **NIST 800-53 r5:** National Institute of Standards and Technology framework
- **PCI DSS:** Payment Card Industry Data Security Standard

- **CIS AWS Foundations Benchmark:** Center for Internet Security guidelines
- **NIST 800-171 r2:** Controlled Unclassified Information protection
- **SOC 2 Type II:** Service Organization Control 2 requirements

This checklist provides systematic coverage across all major AWS services, ensuring no security gaps in your cloud infrastructure.

## ACM (AWS Certificate Manager) Controls

### Certificate Renewal Management

ACM.1

Imported and ACM-issued certificates should be renewed appropriately

□ Set up automatic renewal for ACM-issued certificates

*Prevents service disruption from expired certificates*

□ Monitor expiration dates for imported certificates

*Ensures manual renewal of imported certificates before expiry*

□ Configure CloudWatch alarms for certificate expiration

*Provides early warning for certificate renewal requirements*

NIST 800-53 r5 PCI DSS NIST 800-171 r2

### RSA Key Length Requirements

ACM.2

RSA certificates managed by ACM should use adequate key length

□ Ensure RSA certificates use minimum 2048-bit key length

*Meets cryptographic standards for secure communications*

□ Audit existing certificates for key length compliance

*Identifies certificates that need to be reissued with stronger keys*

PCI DSS

### ACM Certificate Tagging

ACM.3

ACM certificates should be tagged for proper resource management

□ Apply consistent tagging strategy to all certificates

*Enables proper resource management and cost tracking*

□ Include environment, application, and owner tags

*Provides context for certificate usage and ownership*

**NIST 800-53 r5**

# DMS (Database Migration Service) Controls

### DMS Replication Instance Privacy

**DMS.1**

Database Migration Service replication instances should not be public

□ Deploy DMS replication instances in private subnets

*Prevents direct internet access to migration infrastructure*

□ Configure security groups with minimal required access

*Limits network access to only necessary source and target systems*

**NIST 800-53 r5** **PCI DSS**

### DMS Resource Tagging

**DMS.2-5**

DMS resources should be properly tagged

□ Tag DMS certificates with appropriate metadata

*Enables proper certificate lifecycle management*

□ Tag DMS event subscriptions for monitoring

*Provides context for event notification management*

□ Tag DMS replication instances and subnet groups

*Supports resource organization and cost allocation*

## DMS Version Management

DMS.6

DMS replication instances should have automatic minor version upgrade enabled

□ Enable automatic minor version upgrades

*Ensures timely application of security patches*

□ Schedule maintenance windows for upgrades

*Minimizes impact on migration operations*

NIST 800-53 r5 PCI DSS

## DMS Logging Configuration

DMS.7-8

DMS replication tasks should have logging enabled

□ Enable logging for target database replication tasks

*Provides audit trail for data migration activities*

□ Enable logging for source database replication tasks

*Captures source system interactions for troubleshooting*

□ Configure log retention policies

*Balances storage costs with compliance requirements*

NIST 800-53 r5 PCI DSS

## DMS Endpoint Security

DMS.9-12

DMS endpoints should use secure connections

□ Configure SSL/TLS encryption for DMS endpoints

*Encrypts data in transit during migration*

□ Use IAM authorization for Neptune database endpoints

*Provides fine-grained access control to graph databases*

□ Configure authentication for MongoDB endpoints

*Ensures secure access to NoSQL databases*

□ Enable TLS for Redis OSS endpoints

*Secures connections to Redis cache instances*

NIST 800-53 r5 PCI DSS

# EC2 (Elastic Compute Cloud) Controls

## EBS Snapshot Privacy

EC2.1

Amazon EBS snapshots should not be publicly restorable

□ Audit all EBS snapshots for public access
*Prevents unauthorized access to snapshot data*

□ Remove public permissions from snapshots
*Ensures snapshots remain within your control*

NIST 800-53 r5 PCI DSS

## VPC Default Security Groups

EC2.2

VPC default security groups should not allow traffic

□ Remove all inbound rules from default security groups
*Prevents accidental exposure through default configurations*

□ Remove all outbound rules from default security groups
*Enforces explicit security group assignments*

NIST 800-53 r5 PCI DSS CIS AWS Foundations

## EBS Volume Encryption

EC2.3, EC2.7

EBS volumes should be encrypted at rest

□ Enable EBS default encryption
*Automatically encrypts all new EBS volumes*

□ Encrypt existing attached EBS volumes

*Protects data at rest from unauthorized access*

□ Use customer-managed KMS keys where required

*Provides additional key management control*

NIST 800-53 r5 CIS AWS Foundations

### RDS High Availability

RDS.5, RDS.15

RDS instances should be configured for high availability

□ Enable Multi-AZ deployment for RDS instances

*Provides automatic failover and high availability*

□ Configure RDS clusters across multiple Availability Zones

*Ensures cluster resilience and availability*

NIST 800-53 r5

### RDS Monitoring and Logging

RDS.6, RDS.9

RDS should have proper monitoring and logging

□ Enable Enhanced Monitoring for RDS instances

*Provides detailed performance metrics and monitoring*

□ Configure RDS to publish logs to CloudWatch

*Centralizes database logs for monitoring and analysis*

NIST 800-53 r5 PCI DSS

### RDS Backup and Recovery

RDS.11, RDS.14, RDS.26

RDS should have comprehensive backup strategy

□ Enable automated backups for all RDS instances

*Ensures regular backup creation without manual intervention*

□ Enable backtracking for Aurora clusters

*Allows point-in-time recovery without restoring from backup*

□ Protect RDS instances with AWS Backup plans

*Provides centralized backup management and compliance*

NIST 800-53 r5

### RDS Access Control

RDS.10, RDS.12

RDS should use IAM authentication where possible

□ Enable IAM authentication for RDS instances

*Provides centralized access control through IAM*

□ Configure IAM authentication for RDS clusters

*Enables fine-grained access control for cluster resources*

NIST 800-53 r5

### RDS Security Configuration

RDS.13, RDS.23-25

RDS should follow security best practices

□ Enable automatic minor version upgrades

*Ensures timely application of security patches*

□ Use non-default ports for RDS instances

*Reduces exposure to automated port scans*

□ Use custom administrator usernames

*Avoids easily guessable default administrator accounts*

NIST 800-53 r5 PCI DSS CIS AWS Foundations

## S3 (Simple Storage Service) Controls

### S3 Bucket Public Access

S3.1, S3.2, S3.3, S3.8

S3 buckets should block public access

□ Enable Block Public Access settings for all buckets

*Prevents accidental public exposure of bucket contents*

□ Block public read access to bucket contents

*Prevents unauthorized access to sensitive data*

□ Block public write access to buckets

*Prevents unauthorized modification of bucket contents*

**NIST 800-53 r5** **PCI DSS** **CIS AWS Foundations**

## S3 Encryption in Transit

**S3.5**

S3 buckets should require SSL/TLS

□ Implement bucket policies requiring HTTPS

*Ensures all data transmission is encrypted*

□ Deny HTTP requests to S3 buckets

*Prevents unencrypted data transmission*

**NIST 800-53 r5** **NIST 800-171 r2** **PCI DSS** **CIS AWS Foundations**

## S3 Encryption at Rest

**S3.17**

S3 buckets should be encrypted with AWS KMS keys

□ Enable default encryption for all S3 buckets

*Ensures all objects are encrypted at rest*

□ Use customer-managed KMS keys for sensitive data

*Provides additional control over encryption keys*

**NIST 800-53 r5** **NIST 800-171 r2** **PCI DSS**

## S3 Logging and Monitoring

**S3.9, S3.11**

S3 should have comprehensive logging

□ Enable server access logging for all buckets

*Provides audit trail of bucket access*

□ Configure event notifications for bucket activities

*Enables real-time monitoring of bucket operations*

NIST 800-53 r5 NIST 800-171 r2 PCI DSS

### S3 Versioning and Lifecycle

S3.10, S3.13, S3.14

S3 should have proper versioning and lifecycle management

□ Enable versioning for all critical buckets

*Provides protection against accidental deletion or corruption*

□ Configure lifecycle policies for cost optimization

*Automatically manages object storage classes and retention*

□ Set up lifecycle rules for versioned objects

*Prevents unlimited accumulation of object versions*

NIST 800-53 r5 NIST 800-171 r2

### S3 Access Control

S3.6, S3.12

S3 should use proper access control mechanisms

□ Restrict bucket policies to authorized AWS accounts

*Limits cross-account access to trusted entities*

□ Use IAM policies instead of ACLs for access control

*Provides more granular and manageable access control*

NIST 800-53 r5 NIST 800-171 r2

## IAM (Identity and Access Management) Controls

## IAM Policy Restrictions

IAM.1, IAM.21

IAM policies should not allow full administrative privileges

□ Avoid policies with Effect: Allow and Resource: "*"

*Prevents granting excessive permissions*

□ Review customer-managed policies for over-privileges

*Ensures policies follow least privilege principle*

□ Implement conditions in IAM policies

*Adds context-based restrictions to permissions*

NIST 800-53 r5 NIST 800-171 r2 PCI DSS CIS AWS Foundations

## IAM User Management

IAM.2

IAM users should not have policies attached directly

□ Attach policies to groups, not individual users

*Simplifies permission management and reduces errors*

□ Use IAM roles for applications and services

*Provides temporary credentials without long-term keys*

NIST 800-53 r5 NIST 800-171 r2 PCI DSS CIS AWS Foundations

## IAM Access Key Management

IAM.3, IAM.8, IAM.22

IAM access keys should be properly managed

□ Rotate access keys every 90 days

*Limits exposure window if keys are compromised*

□ Remove unused credentials and access keys

*Eliminates unnecessary attack vectors*

□ Identify and remove unused user credentials (45+ days)

*Reduces risk from dormant accounts*

NIST 800-53 r5 NIST 800-171 r2 PCI DSS CIS AWS Foundations

## Root Account Security

IAM.4, IAM.6, IAM.9, IAM.20

Root account should be secured and not used regularly

□ Remove all access keys from root account

*Eliminates programmatic access to most powerful account*

□ Enable hardware MFA for root account

*Provides strongest authentication for root access*

□ Avoid using root account for daily operations

*Limits exposure of most privileged account*

NIST 800-53 r5 PCI DSS CIS AWS Foundations

## Multi-Factor Authentication

IAM.5, IAM.19

MFA should be enabled for all users

□ Enable MFA for all users with console passwords

*Adds second factor authentication for console access*

□ Require MFA for all IAM users

*Provides comprehensive multi-factor authentication*

NIST 800-53 r5 NIST 800-171 r2 PCI DSS CIS AWS Foundations

## Password Policy

IAM.7, IAM.10-17

IAM password policy should be comprehensive

□ Require minimum 14-character passwords

*Increases resistance to brute force attacks*

□ Require uppercase, lowercase, numbers, and symbols

*Increases password complexity and entropy*

□ Prevent password reuse (last 24 passwords)

*Forces users to create new passwords*

□ Set password expiration (90 days or less)

*Limits exposure window of compromised passwords*

NIST 800-53 r5 NIST 800-171 r2 PCI DSS CIS AWS Foundations

### IAM Support Role

IAM.18

Support role should be created for incident management

□ Create IAM role for AWS Support access

*Enables efficient incident response with AWS Support*

□ Assign Support role to incident response team

*Ensures proper access during security incidents*

NIST 800-171 r2 PCI DSS CIS AWS Foundations

### IAM Access Analyzer

IAM.28

IAM Access Analyzer should be enabled

□ Enable IAM Access Analyzer in all regions

*Identifies resources shared with external entities*

□ Review and remediate Access Analyzer findings

*Addresses unintended external access to resources*

CIS AWS Foundations

## Additional Service Controls

### KMS Key Management

KMS.1-5

KMS keys should be properly managed

□ Restrict IAM policies from decrypting all KMS keys

*Prevents overly broad decryption permissions*

□ Avoid granting decrypt permissions on all keys

*Follows principle of least privilege for encryption*

□ Enable automatic key rotation

*Regularly rotates encryption keys for security*

□ Ensure KMS keys are not publicly accessible

*Prevents unauthorized access to encryption keys*

**NIST 800-53 r5** **PCI DSS** **CIS AWS Foundations**

## CloudTrail Configuration

**CloudTrail.1-5**

CloudTrail should be properly configured

□ Enable CloudTrail in all regions

*Provides comprehensive API logging across all regions*

□ Enable log file validation

*Detects tampering with CloudTrail logs*

□ Encrypt CloudTrail logs with KMS

*Protects audit logs from unauthorized access*

**NIST 800-53 r5** **PCI DSS** **CIS AWS Foundations**

## GuardDuty Threat Detection

**GuardDuty.1**

GuardDuty should be enabled for threat detection

□ Enable GuardDuty in all regions

*Provides AI-powered threat detection globally*

□ Configure GuardDuty findings notifications

*Ensures prompt response to security threats*

□ Enable GuardDuty S3 protection

*Monitors S3 buckets for malicious activity*

NIST 800-53 r5

## Systems Manager

SSM.1-5

Systems Manager should be properly configured

□ Manage EC2 instances with Systems Manager

*Provides centralized instance management and patching*

□ Configure patch compliance for managed instances

*Ensures instances receive security updates*

□ Ensure SSM documents are not public

*Prevents unauthorized access to automation scripts*

NIST 800-53 r5 PCI DSS

## Load Balancer Security

ELB.1-17

Load balancers should be securely configured

□ Redirect HTTP traffic to HTTPS

*Ensures all traffic is encrypted in transit*

□ Use predefined security policies for SSL/TLS

*Ensures strong encryption protocols*

□ Enable access logging for load balancers

*Provides audit trail for load balancer access*

□ Configure load balancers across multiple AZs

*Ensures high availability and fault tolerance*

NIST 800-53 r5 NIST 800-171 r2 PCI DSS

## WAF Configuration

WAF.1-12

WAF should be properly configured

□ Enable logging for WAF web ACLs

*Provides visibility into web application attacks*

□ Configure WAF rules for web ACLs

*Provides protection against common web attacks*

□ Enable CloudWatch metrics for WAF rules

*Monitors WAF performance and effectiveness*

NIST 800-53 r5 PCI DSS

## Next Steps

**1. Assessment:** Use this comprehensive checklist to evaluate your complete AWS security posture across all services

**2. Prioritization:** Focus on high-impact controls first, particularly those mapped to your compliance requirements

**3. Implementation:** Work through controls systematically, documenting configurations and exceptions

**4. Automation:** Implement continuous monitoring to ensure configurations remain compliant over time

**5. Documentation:** Maintain evidence of compliance for audit and regulatory requirements

### Instance Lifecycle Management

EC2.4

Stopped EC2 instances should be removed after specified time

□ Implement automated cleanup of stopped instances

*Reduces costs and attack surface*

□ Define retention policies for stopped instances

*Provides clear guidelines for resource cleanup*

NIST 800-53 r5

## VPC Flow Logs

EC2.6

VPC flow logging should be enabled in all VPCs

□ Enable VPC Flow Logs for all VPCs

*Provides network traffic visibility for security monitoring*

□ Configure flow logs to capture all traffic

*Ensures comprehensive network monitoring*

NIST 800-53 r5 NIST 800-171 r2 PCI DSS CIS AWS Foundations

## Instance Metadata Service

EC2.8

EC2 instances should use IMDSv2

□ Configure all instances to require IMDSv2

*Prevents SSRF attacks against instance metadata*

□ Disable IMDSv1 on all instances

*Eliminates vulnerable legacy metadata access*

NIST 800-53 r5 PCI DSS CIS AWS Foundations

## Instance Network Exposure

EC2.9, EC2.15, EC2.25

EC2 instances should not have unnecessary public IP addresses

□ Remove public IP addresses from instances that don't need them

*Reduces internet exposure and attack surface*

□ Configure subnets to not auto-assign public IPs

*Prevents accidental public exposure of new instances*

□ Update launch templates to avoid public IP assignment

*Ensures consistent private deployment patterns*

NIST 800-53 r5 PCI DSS

## VPC Endpoints

EC2.10

EC2 should use VPC endpoints for AWS services

□ Create VPC endpoints for commonly used AWS services

*Keeps traffic within AWS network infrastructure*

□ Configure endpoint policies for access control

*Limits which resources can use the endpoints*

**NIST 800-53 r5** **NIST 800-171 r2**

## Security Group Configuration

EC2.13, EC2.14, EC2.18, EC2.19

Security groups should follow least privilege principles

□ Remove rules allowing 0.0.0.0/0 access to SSH (port 22)

*Prevents global SSH access and brute force attacks*

□ Remove rules allowing 0.0.0.0/0 access to RDP (port 3389)

*Blocks worldwide remote desktop access*

□ Restrict unrestricted access to authorized ports only

*Limits public exposure to necessary services*

□ Block unrestricted access to high-risk ports

*Prevents exploitation of commonly attacked services*

**NIST 800-53 r5** **NIST 800-171 r2** **PCI DSS** **CIS AWS Foundations**

## Network Access Control Lists

EC2.21

Network ACLs should not allow unrestricted access

□ Remove NACL rules allowing 0.0.0.0/0 to SSH/RDP

*Provides subnet-level protection against remote access*

□ Implement deny-by-default NACL policies

*Requires explicit permission for network access*

NIST 800-53 r5 NIST 800-171 r2 PCI DSS CIS AWS Foundations

## VPN Connection Redundancy

EC2.20

Site-to-Site VPN connections should have both tunnels up

□ Monitor VPN tunnel status

*Ensures high availability of site-to-site connections*

□ Configure alerts for tunnel failures

*Provides immediate notification of connectivity issues*

NIST 800-53 r5 NIST 800-171 r2

## EC2 Resource Management

EC2.12, EC2.16, EC2.22

Remove unused EC2 resources

□ Release unused Elastic IP addresses

*Reduces costs and potential attack vectors*

□ Remove unused Network Access Control Lists

*Simplifies network security management*

□ Delete unused security groups

*Reduces configuration complexity and potential misuse*

NIST 800-53 r5 NIST 800-171 r2 PCI DSS

## EC2 Resource Tagging

EC2.33-52

EC2 resources should be properly tagged

□ Apply consistent tagging to all EC2 resources

*Enables proper resource management and cost allocation*

□ Include mandatory tags: Environment, Application, Owner

*Provides essential metadata for resource governance*

□ Tag all resource types: instances, volumes, networks, etc.

*Ensures comprehensive resource visibility*

# ECS (Elastic Container Service) Controls

## ECS Task Definition Security

ECS.1

ECS task definitions should have secure networking modes

□ Configure task definitions with appropriate user permissions

*Prevents containers from running with excessive privileges*

□ Use bridge or awsvpc networking modes

*Provides network isolation for containerized applications*

NIST 800-53 r5

## ECS Service Network Security

ECS.2

ECS services should not have public IP addresses

□ Deploy ECS services in private subnets

*Prevents direct internet access to container services*

□ Use load balancers for public access when needed

*Provides controlled access through dedicated infrastructure*

NIST 800-53 r5 PCI DSS

## Container Runtime Security

ECS.3-5

ECS containers should follow security best practices

□ Avoid sharing host process namespace

*Isolates container processes from host system*

□ Run containers as non-privileged users

*Limits potential damage from container compromise*

□ Set containers to read-only root filesystems

*Prevents runtime modifications to container filesystems*

NIST 800-53 r5

### ECS Secrets Management

ECS.8

Secrets should not be passed as environment variables

□ Use AWS Secrets Manager for sensitive data

*Provides secure storage and rotation of secrets*

□ Remove hardcoded secrets from task definitions

*Prevents exposure of sensitive information*

NIST 800-53 r5 PCI DSS

### ECS Logging and Monitoring

ECS.9, ECS.12

ECS should have proper logging and monitoring

□ Configure logging for all task definitions

*Provides audit trail and troubleshooting capabilities*

□ Enable Container Insights for ECS clusters

*Provides enhanced monitoring and performance metrics*

NIST 800-53 r5

## EKS (Elastic Kubernetes Service) Controls

### EKS Cluster Network Security

EKS.1

EKS cluster endpoints should not be publicly accessible

□ Configure EKS cluster endpoints as private

*Prevents direct internet access to Kubernetes API*

□ Use bastion hosts or VPN for cluster access

*Provides secure access path to private clusters*

NIST 800-53 r5 PCI DSS

## EKS Version Management

EKS.2

EKS clusters should run supported Kubernetes versions

□ Maintain EKS clusters on supported Kubernetes versions

*Ensures access to security patches and support*

□ Plan regular cluster upgrades

*Prevents running on deprecated versions*

NIST 800-53 r5 PCI DSS

## EKS Secrets Encryption

EKS.3

EKS clusters should use encrypted Kubernetes secrets

□ Enable envelope encryption for Kubernetes secrets

*Protects sensitive data stored in etcd*

□ Use customer-managed KMS keys for encryption

*Provides additional control over encryption keys*

NIST 800-53 r5 PCI DSS

## EKS Audit Logging

EKS.8

EKS clusters should have audit logging enabled

□ Enable EKS control plane logging

*Provides audit trail for cluster API activities*

□ Configure log types: API, audit, authenticator

*Captures comprehensive cluster activity*

NIST 800-53 r5 PCI DSS

# RDS (Relational Database Service) Controls

## RDS Snapshot Security

RDS.1

RDS snapshots should be private

□ Audit all RDS snapshots for public access

*Prevents unauthorized access to database backups*

□ Remove public permissions from snapshots

*Ensures database backups remain private*

NIST 800-53 r5 PCI DSS

## RDS Public Access

RDS.2

RDS instances should not be publicly accessible

□ Configure RDS instances with public access disabled

*Prevents direct internet access to databases*

□ Deploy RDS instances in private subnets

*Provides network-level isolation for databases*

NIST 800-53 r5 PCI DSS CIS AWS Foundations

## RDS Encryption

RDS.3, RDS.4, RDS.27

RDS instances should be encrypted at rest

□ Enable encryption for all RDS instances

*Protects database data from unauthorized access*

□ Encrypt RDS snapshots and cluster snapshots

*Ensures backup data is also protected*

□ Enable encryption for RDS clusters

*Protects multi-instance database configurations*

**NIST 800-53 r5** **CIS AWS Foundations**

## Need Help Managing These 300+ Security Controls?

Manual implementation and monitoring of hundreds of security controls is complex and time-consuming. Enterprise-grade Cloud Security Posture Management (CSPM) solutions provide automated, continuous monitoring of your entire AWS environment with real-time compliance reporting, executive dashboards, and automated remediation capabilities.

**AWSight** provides comprehensive coverage of all AWS Foundational Security Best Practices with intelligent prioritization, compliance mapping, and actionable remediation guidance designed for growing businesses.

Transform your security management from reactive to proactive. Visit awsight.com to see how automated security monitoring can protect your business while enabling rapid growth and innovation.

## Need Help Managing These 300+ Security Controls?

Manual implementation and monitoring of hundreds of security controls is complex and time-consuming. Enterprise-grade Cloud Security Posture Management (CSPM) solutions provide automated, continuous monitoring of your entire AWS environment with real-time compliance reporting, executive dashboards, and automated remediation capabilities.

**AWSight** provides comprehensive coverage of all AWS Foundational Security Best Practices with intelligent prioritization, compliance mapping, and actionable remediation guidance designed for growing businesses.

Transform your security management from reactive to proactive. Visit **awsight.com** to see how automated security monitoring can protect your business while enabling rapid growth and innovation.