Provided by:



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 by Standard

Complete Controls Guide Mapped to Compliance
Frameworks

A comprehensive security checklist organized by compliance standard, mapping all AWS Foundational Security Best Practices to CIS AWS Foundations Benchmark, NIST 800-53 r5, NIST 800-171 r2, and PCI DSS requirements for streamlined audit preparation.

300+

5

100%

AWS Security Controls

Compliance Standards

Framework Coverage

Why Compliance-Mapped Security Matters

Organizations face increasing regulatory pressure to demonstrate security compliance across multiple frameworks. This checklist organizes AWS security controls by compliance standard, making it easier to prepare for audits and maintain continuous compliance.

This guide maps AWS Foundational Security Best Practices to:

• **CIS AWS Foundations Benchmark:** Center for Internet Security's authoritative security configuration guidelines

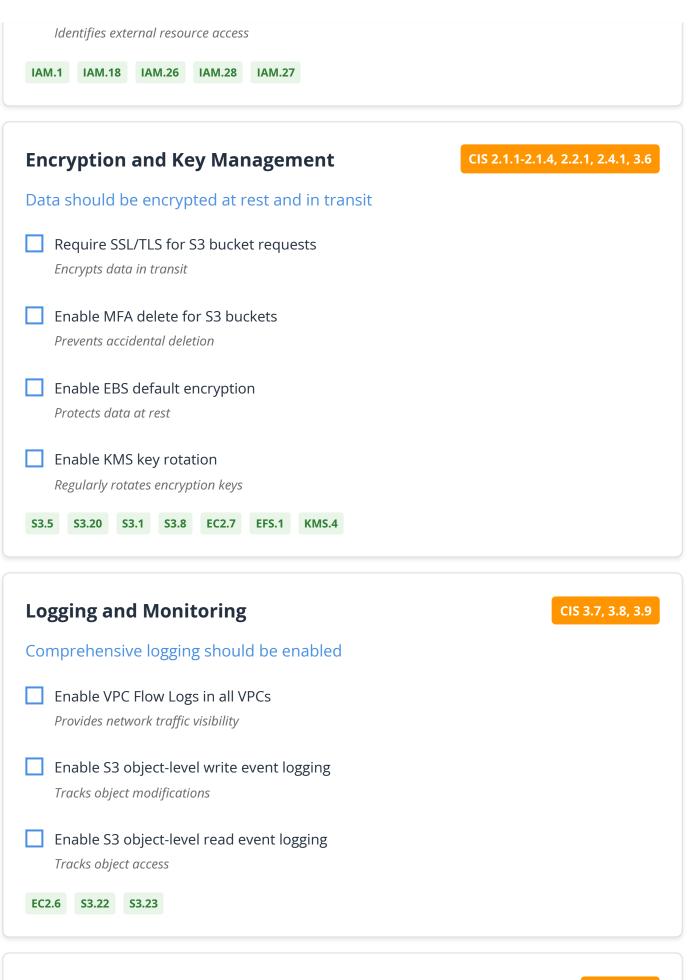
- NIST 800-53 r5: National Institute of Standards and Technology's comprehensive security framework
- NIST 800-171 r2: Controlled Unclassified Information (CUI) protection requirements
- PCI DSS v3.2.1 & v4.0.1: Payment Card Industry Data Security Standards

Each compliance requirement is linked to specific AWS controls, enabling targeted implementation and efficient audit preparation. Organizations can focus on controls that satisfy multiple compliance obligations simultaneously.

CIS AWS Foundations Benchmark

Root Account Security CIS 1.1, 1.4, 1.5, 1.6 Root user should be secured and not used for daily operations Avoid using root user for daily operations Reduces exposure of most privileged account Remove access keys from root account Eliminates programmatic access to root Enable MFA for root user Provides multi-factor authentication protection Enable hardware MFA for root user Provides strongest authentication method IAM.20 IAM.4 IAM.9 IAM.6 CIS 1.2, 1.3, 1.10, 1.12, 1.14, 1.15, 1.16 IAM User Management IAM users should follow security best practices Enable MFA for all IAM users with console passwords Adds second factor authentication Remove unused IAM user credentials

Eliminates dormant security risks
Rotate access keys every 90 days
Limits exposure window if compromised
Attach policies to groups, not users directly
Attach policies to groups, not users directly Simplifies permission management
IAM.5 IAM.8 IAM.3 IAM.22 IAM.2
IAM Password Policy CIS 1.5-1.11
Password policy should enforce strong requirements
Require minimum 14-character passwords
Increases resistance to brute force attacks
Require uppercase, lowercase, numbers, and symbols
Increases password complexity
<u> </u>
Prevent password reuse
Forces users to create new passwords
Set password expiration within 90 days
Limits exposure window
IAM.15 IAM.11 IAM.12 IAM.13 IAM.14 IAM.16 IAM.17
IAM Policy Management CIS 1.16, 1.17, 1.19, 1.20, 1.22
IAM policies should follow least privilege principles
Avoid policies with full administrative privileges
Prevents excessive permissions
Croate support role for AWS incident management
Create support role for AWS incident management Enables efficient incident response
Remove expired SSL/TLS certificates
Eliminates security vulnerabilities
Enable IAM Access Analyzer



Network Security

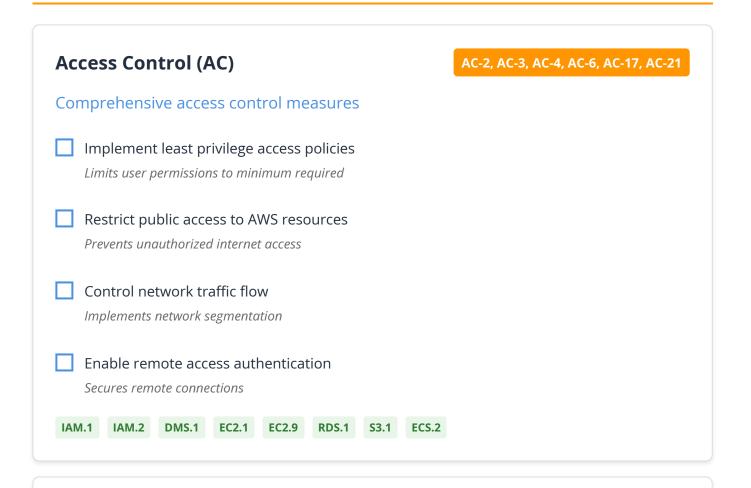
CIS 5.1-5.6

Network access should be properly restricted

Restrict NACL access to SSH and RDP ports Provides subnet-level protection
Restrict security group access to remote server ports Blocks worldwide remote access
Configure default security groups to deny all traffic Prevents accidental exposure
Use Instance Metadata Service Version 2 Prevents SSRF attacks
EC2.21 EC2.53 EC2.54 EC2.2 EC2.8 EC2.171

NIS

NIST 800-53 r5



Audit and Accountability (AU)

AU-2, AU-3, AU-6, AU-9, AU-10, AU-12

Comprehensive audit logging and monitoring

Enable comprehensive audit logging

Prov	vides acco	ountability	and for	ensic cap	oabilities							
		lit logs fr		npering	;							
		d analyz ly threat a		records	5							
		log aggr	_	and co	orrelatio	n						
DMS.7	DMS.8	EC2.51	ECS.9	EKS.8	RDS.9	S3.9	WAF.1					
Config Secure		on Ma				ces		O	CM-2, C	M-3, CN	Л-7, СМ-8	
		aseline c										
		ifiguratio uthorized		_								
		least fur		ity prin	ciple							
		formation	-	m com	ponent	invento	ory					
EC2.4	ECS.3	ELB.6	RDS.7	EC2.12	SSM.1							
Conti	ngenc	y Plan	ning	(CP)						СР-6, СР	P-9, CP-10	
Data ba	ackup a	nd reco	overy c	apabili	ties							
		compre recovery			p strateg	gy						
		and rec		orocedu	ures							
☐ Imp	lement	redunda	ancy an	d high a	availabil	ity						

Ensures service continuity							
EC2.28 EFS.2 RDS.11 RDS.26 S3.14 S3.7 ELB.10 RDS.5							
System and Communications Protection (SC) SC-7, SC-8, SC-12, SC-13, SC-28							
Cryptographic protection and secure communications							
Implement boundary protection Controls network access points							
Encrypt data in transit Protects data during transmission							
Implement cryptographic key management Secures encryption keys							
Encrypt data at rest							
Protects stored data EC2.13 EC2.2 DMS.9 ELB.1 KMS.3 KMS.4 EC2.3 RDS.3 S3.17							
ECZ.13 ECZ.2 DIVIS.9 ELD.1 RIVIS.3 RIVIS.4 ECZ.3 RDS.3 SS.17							
System and Information Integrity (SI)							
System and Information Integrity (SI) System and Information Integrity (SI) System and Information Integrity (SI)							
System integrity monitoring and flaw remediation							
Implement flaw remediation processes Ensures timely security updates							
Deploy malicious code protection Prevents malware infections							
Monitor system security events Enables threat detection							
Implement information backup and recovery Ensures data resilience							
DMS.6 ECS.10 RDS.13 SSM.2 S3.11 EC2.28 RDS.5							

Access Control (3.1)	3.1.1, 3.1.2, 3.1.3, 3.1.4, 3.1.5, 3.1.7
Controlled Unclassified Information (CUI) access control	ol
Limit system access to authorized users Protects CUI from unauthorized access	
Limit system access to authorized processes Controls programmatic access to CUI	
Control information flows within systems Prevents unauthorized data movement	
Separate duties of individuals Reduces risk of insider threats	
IAM.21 IAM.2 EC2.10 EC2.13 EC2.18 IAM.1 IAM.22	
Awareness and Training (3.2)	3.2.1, 3.2.2, 3.2.3
Security awareness and training programs	
Ensure personnel receive security awareness training Reduces human error security risks	
Ensure personnel receive role-based training Provides targeted security knowledge	
Document security training activities Demonstrates compliance efforts	

Audit and Accountability (3.3)

3.3.1, 3.3.8, 3.3.9

Audit capabilities for CUI systems

Create and retain audit records									
Provides accountability for CUI access									
Protect audit information and tools									
Ensures audit trail integrity									
Limit management of audit functionality									
Prevents audit tampering									
EC2.6 IAM.19 S3.11 S3.9 S3.14 IAM.21									
Configuration Management (3.4) 3.4.1, 3.4.2, 3.4.6, 3.4.7, 3.4.8, 3.4.9									
Secure configuration management for CUI systems									
Establish configuration baselines									
Ensures consistent secure configurations									
Control and monitor configuration changes									
Prevents unauthorized modifications									
Employ least functionality principle									
Reduces attack surface									
Restrict software installation									
Prevents unauthorized software									
EC2.16									
Identification and Authentication (3.5) 3.5.1, 3.5.2, 3.5.3, 3.5.4, 3.5.7, 3.5.8, 3.5.9									
User identification and authentication for CUI access									
Identify users before granting access									
Ensures accountability for CUI access									
Authenticate users before granting access									
Verifies user identity									
Use multi-factor authentication									
Provides strong authentication									

Employ strong Ensures passwor	g password polic	cies			
AM.10 IAM.11	IAM.12 IAM.13	IAM.14 IAM.15	IAM.16	IAM.17	IAM.19
	_		_		
	Communicat	tions Protec	tion	3.13.1, 3 3.13.16	3.13.8, 3.13.11, 3.13.15
ystem and C 3.13) rotection of CU			tion		3.13.8, 3.13.11, 3.13.15
3.13) rotection of CU Monitor comn		l at rest xternal boundar			3.13.8, 3.13.11, 3.13.15

Protects stored CUI

Protect CUI in transit

Encrypt CUI at rest

Secures CUI during transmission

EC2.10 EC2.13 S3.17 SNS.1 ELB.3 S3.5

PCI DSS v3.2.1 & v4.0.1

Network Security (Requirements 1-2)	1.2.1, 1.3.1, 1.3.2, 1.3.4, 1.3.6, 1.4.4, 2.1, 2.2
Network security controls for cardholder data p	rotection
Install and maintain firewall configuration Protects cardholder data networks	
Restrict network access to cardholder data Limits exposure of sensitive data	
Remove default security parameters Eliminates known vulnerabilities	

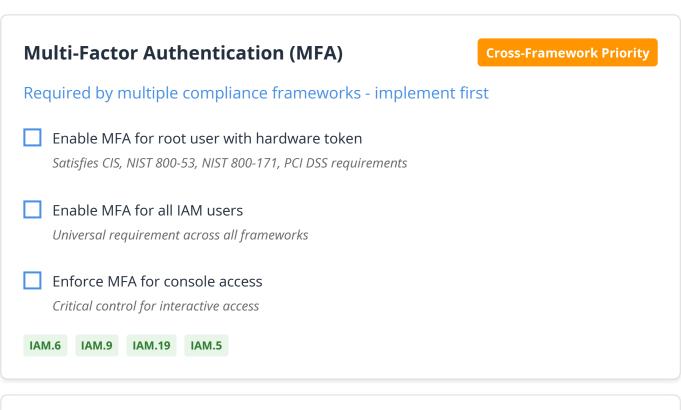
Implement network segmentation Isolates cardholder data environment
DMS.1 EC2.1 EC2.2 EC2.13 EMR.1 RDS.1 RDS.2 S3.1 S3.2 S3.3
Data Protection (Requirements 3-4) 3.4, 3.6.4, 3.7.4, 4.1, 4.2.1
Protect stored cardholder data and encrypt transmission
Protect stored cardholder data
Prevents unauthorized access to sensitive data
Encrypt cardholder data transmission Protects data in transit
Implement cryptographic key management Secures encryption keys
ES.1 KMS.4 ELB.1 S3.5 ACM.1 ACM.2 DMS.9 ELB.3
Access Control 7.2.1, 7.3.1, 8.1.4, 8.2.3, 8.2.4, 8.2.5, 8.2.6, 8.3.1, 8.3.2, 8.3.6,
(Requirements 7-8) 8.3.7, 8.3.9, 8.4.2, 8.6.2, 8.6.3
Restrict access to cardholder data by business need-to-know
Restrict access to cardholder data
Limits exposure based on business need
Assign unique ID to each person with access Ensures accountability
Implement strong authentication measures Verifies user identity
Implement multi-factor authentication Provides additional security layer
EC2.1 IAM.1 IAM.2 IAM.4 IAM.8 IAM.10 IAM.11 IAM.12 IAM.13 IAM.14 IAM.16
IAM.17 IAM.19 IAM.5 IAM.6 IAM.9 ECS.8

vuinerabi	lity Mar	nagen	nent (Requi	ii Ciiic	ent 6)		0.	.2, 6.2.	3, 6.2.4, 6.3.3
Develop and maintain secure systems and applications										
	urity patch		-	anner						
	vulnerabilit ecurity weak	-	ning							
	eb applica ainst applica									
	ems and s		e up to c	date						
SSM.2 ECR.1	ELB.12	ELB.4	ELB.14	DMS.6	ECS.10	MQ.3	RDS.1	3 RDS	5.35	SSM.3
Monitorin 11)	g and L	oggin	g (Red	quirer	nents	s 10-	10.2.1 11.5.2	, 10.3.3,	10.4.2	2, 10.5.1,
	onitor all	access	to net	-				, 10.3.3,	. 10.4.2	2, 10.5.1,
11)Track and mLog all acceptodes auImplement	onitor all	access rdholder sensitive	to net	-				, 10.3.3,	10.4.2	2, 10.5.1,
11) Track and m Log all acceptoides au Implement Detects sus Secure log	onitor all cess to car udit trail for nt log mon picious activ	access rdholder sensitive iitoring vities	to net	-				, 10.3.3,	10.4.2	2, 10.5.1,
11) Track and m Log all acceptoides au Implement Detects sus Secure log Prevents log Test secure	onitor all cess to car udit trail for nt log mon picious activ	access rdholder sensitive hitoring vities	to net	-				, 10.3.3,	10.4.2	2, 10.5.1,
11) Track and m Log all acceptoides au Implement Detects sus Secure log Prevents log Test secure	onitor all cess to car udit trail for nt log mon picious activ g data g tampering rity system ecurity contr	access rdholder sensitive hitoring vities	to net	-	esource	es	11.5.2	, 10.3.3,	10.4.2	
Track and m Log all accentrates and m Implement Detects sus Secure log Prevents log Test secur Validates se	onitor all cess to car udit trail for nt log mon picious activ g data g tampering rity system ecurity contr	access rdholder sensitive hitoring vities rs regular rols effect	to net	work re	esource	es	11.5.2			

Maintain policy that addresses information security

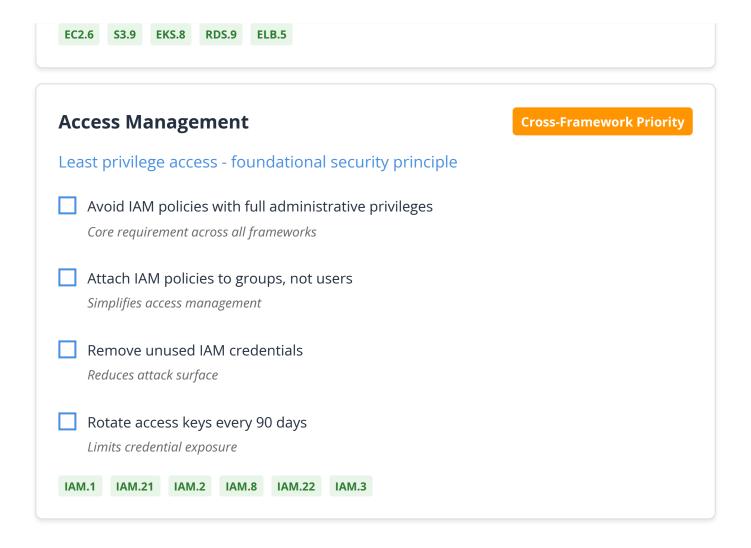
Maintain security policies and procedures Establishes security governance framework	
Implement incident response procedures Ensures timely response to security events	
Conduct regular security training Maintains security awareness	
EKS.2 IAM.18	

High-Impact Cross-Framework Controls



Data Encryption	Cross-Framework Priority
Encryption at rest and in transit - mandatory for most fran	
Enable EBS default encryption Protects all storage volumes automatically	
Require HTTPS for all S3 bucket requests Encrypts data in transit universally	
Encrypt RDS instances and snapshots	

Protects database data at rest
Enable KMS key rotation
Maintains cryptographic hygiene
EC2.7 S3.5 RDS.3 RDS.27 S3.17 KMS.4
Network Access Control Cross-Framework Priority
Restrict network access - fundamental security control
Block public access to all S3 buckets
Prevents data exposure across all frameworks
Restrict security group access to SSH/RDP
Critical for all compliance requirements
Deploy resources in private subnets
Fundamental network security principle
Configure VPC default security groups to deny all
Prevents accidental exposure
S3.1 S3.8 EC2.13 EC2.14 EC2.9 RDS.2 EC2.2
Audit Logging
Audit Logging Cross-Framework Priority
Comprehensive logging - required by all frameworks
Enable VPC Flow Logs
Network monitoring for all frameworks
Enable CloudTrail in all regions
 Enable CloudTrail in all regions API logging for accountability Configure S3 server access logging
Enable CloudTrail in all regions API logging for accountability
 Enable CloudTrail in all regions API logging for accountability Configure S3 server access logging Object access audit trail Enable EKS audit logging
 Enable CloudTrail in all regions API logging for accountability Configure S3 server access logging Object access audit trail



Compliance Implementation Strategy

Phase 1: Foundation (Weeks 1-2)	Quick Wins
Implement high-impact controls that satisfy multiple frameworks	
Enable MFA for all users (IAM.5, IAM.6, IAM.9, IAM.19) Satisfies requirements across CIS, NIST, and PCI DSS	
Remove root user access keys (IAM.4) Critical for CIS and PCI DSS compliance	
Enable EBS default encryption (EC2.7) Addresses encryption requirements across all frameworks	
Block S3 public access (S3.1, S3.8) Prevents data exposure for all compliance requirements	

Phase 2: Core Controls (Weeks 3-6) Essential Security
Implement logging, monitoring, and network security controls
Enable VPC Flow Logs (EC2.6) Required for NIST 800-53, NIST 800-171, PCI DSS monitoring
Configure security groups (EC2.13, EC2.14) Network access control for CIS and PCI DSS
Require HTTPS for S3 (S3.5) Encryption in transit for NIST and PCI DSS
Enable CloudTrail logging API audit logging for all frameworks
Phase 3: Advanced Controls (Weeks 7-12) Comprehensive Security
Implement remaining controls for full compliance
Configure password policies (IAM.10-17) Identity management for CIS, NIST 800-171, PCI DSS
Enable database encryption (RDS.3, RDS.27) Data protection for NIST and PCI DSS
Implement backup strategies (RDS.11, EC2.28) Business continuity for NIST 800-53
Deploy vulnerability scanning (ECR.1) Security assessment for PCI DSS
Phase 4: Continuous Monitoring (Ongoing) Operational Excellence
Maintain compliance through automation and monitoring
Automate compliance checking Ensures continuous compliance across all frameworks

Implement automated remediation	
Reduces manual effort and compliance gaps	
Regular compliance reporting	
Demonstrates ongoing compliance to auditors	
Update controls for new requirements	
Maintains compliance as frameworks evolve	

Accelerate Your Compliance Journey

Manual tracking of 300+ security controls across multiple compliance frameworks is complex and error-prone. Organizations need automated solutions that provide real-time compliance monitoring, executive dashboards, and audit-ready documentation.

AWSight provides comprehensive Cloud Security Posture Management (CSPM) with complete coverage of all compliance frameworks, intelligent control prioritization, and automated evidence collection designed for growing businesses.

Transform your compliance program from reactive to proactive. Visit <u>awsight.com</u> to see how automated compliance monitoring can streamline your audit preparation and reduce compliance overhead.

Compliance Success Framework

- **1. Prioritization:** Focus on high-impact controls that satisfy multiple frameworks simultaneously
 - **2. Phased Implementation:** Roll out controls systematically to avoid overwhelming your team
 - **3. Documentation:** Maintain comprehensive evidence collection for audit readiness

- 4. Automation: Implement continuous monitoring to ensure ongoing compliance
 - **5. Training:** Educate your team on compliance requirements and security best practices

Remember: Compliance is not a destination but a journey. Regular assessment and improvement of your security posture ensures not just regulatory compliance but genuine protection of your organization's assets and customer data.