PLATOPS

Assess your cloud security posture

PlatOps provides security-first DevOps, cloud, and managed IT services for small and mid-sized businesses. We help organizations achieve compliance certifications, secure their infrastructure, and modernize their operations — without the enterprise price tag.

From SOC 2 and HIPAA compliance to cloud migrations and 24/7 monitoring, our team of engineers delivers measurable results with a 100% audit pass rate across 60+ client engagements.

100%	60+	8-12 wk	24/7
AUDIT PASS RATE	ORGANIZATIONS	AVG. TO COMPLIANCE	MONITORING

Cloud Security Assessment

AWS, Azure & GCP Security Posture Evaluation

Prepared by PlatOps Security Version 1.0 | January 2026

ASSESSMENT OVERVIEW

ATTRIBUTE	VALUE
Total Questions	55
Categories	IAM, Network, Data, Compute, Monitoring, Compliance
Time to Complete	30-45 minutes
Scoring	0-3 per question
Output	Cloud security score + misconfig risk level + priority fixes

Scoring Guide

- **0** = Not implemented / Don't know
- **1** = Partially implemented
- **2** = Mostly implemented
- **3** = Fully implemented with automation

 | 4701 Sangamore Road, Suite 100N #2000, Bethesda, MD 20816
hello@platops.com | (202) 864-1197 | platops.com

FIELD	RESPONSE
Organization Name	
Primary Cloud Provider	[ ] AWS [ ] Azure [ ] GCP [ ] Multi-cloud
Number of Cloud Accounts/Subscriptions	
Production Workloads	[ ] Yes [ ] No
Sensitive Data in Cloud	[ ] PII [ ] PHI [ ] PCI [ ] None
Cloud Security Tool (CSPM)	
Last Security Review Date	

SECTION 1: IDENTITY & ACCESS MANAGEMENT (12 Questions)

1.1 Root/Admin Account Security

#	QUESTION	SCORE (0-3)	CLOUD PROVIDER NOTES
1	Is the root/owner account secured with MFA?	_____	AWS: Root, Azure: Global Admin, GCP: Super Admin
2	Is the root/owner account NOT used for daily operations?	_____	Should only be for account-level changes
3	Are root access keys disabled (AWS) or API access limited?	_____	

Subsection Score: _____ / 9

1.2 IAM Policies & Users

#	QUESTION	SCORE (0-3)	NOTES
4	Is MFA enforced for all human users?	_____	
5	Are IAM policies following least privilege principle?	_____	
6	Are there no wildcard (*) permissions in production?	_____	
7	Is there a process for regular access reviews?	_____	
8	Is user access removed within 24 hours of termination?	_____	

Subsection Score: _____ / 15

#	QUESTION	SCORE (0-3)	NOTES
9	Are service accounts using roles (not access keys) where possible?	_____	
10	Are access keys rotated at least every 90 days?	_____	
11	Is cross-account access properly controlled?	_____	
12	Is federated identity (SSO) used for console access?	_____	

Subsection Score: _____ / 12

IAM TOTAL: _____ / 36

SECTION 2: NETWORK SECURITY (10 Questions)

2.1 VPC/Network Configuration

#	QUESTION	SCORE (0-3)	NOTES
13	Are production workloads in private subnets?	_____	
14	Is network segmentation implemented (prod/dev/staging)?	_____	
15	Are default VPCs/networks not used for production?	_____	
16	Is VPC flow logging enabled?	_____	

Subsection Score: _____ / 12

2.2 Security Groups & Firewalls

#	QUESTION	SCORE (0-3)	NOTES
17	Are security groups following least privilege (no 0.0.0.0/0 inbound)?	_____	
18	Is SSH/RDP restricted to specific IPs or VPN only?	_____	
19	Are unused security groups removed?	_____	
20	Is there a web application firewall (WAF) for public apps?	_____	

Subsection Score: _____ / 12

2.3 Connectivity

#	QUESTION	SCORE (0-3)	NOTES
21	Is private connectivity used for cloud services (VPC endpoints, Private Link)?	_____	
22	Is DDoS protection enabled for public resources?	_____	

Subsection Score: _____ / 6

NETWORK TOTAL: _____ / 30

3.1 Storage Security

#	QUESTION	SCORE (0-3)	NOTES
23	Are storage buckets/blobs NOT publicly accessible?	_____	AWS S3, Azure Blob, GCP Cloud Storage
24	Is public access blocked at the account/subscription level?	_____	
25	Is server-side encryption enabled for all storage?	_____	
26	Is versioning enabled for critical data?	_____	

Subsection Score: _____ / 12

3.2 Database Security

#	QUESTION	SCORE (0-3)	NOTES
27	Are databases encrypted at rest?	_____	RDS, Azure SQL, Cloud SQL
28	Are databases in private subnets (not publicly accessible)?	_____	
29	Is encryption in transit enforced for database connections?	_____	
30	Are database backups encrypted?	_____	

Subsection Score: _____ / 12

3.3 Key Management

#	QUESTION	SCORE (0-3)	NOTES
31	Is a managed key service used (KMS)?	_____	AWS KMS, Azure Key Vault, GCP KMS
32	Are customer-managed keys used for sensitive data?	_____	

Subsection Score: _____ / 6

DATA PROTECTION TOTAL: _____ / 30

SECTION 4: COMPUTE SECURITY (8 Questions)

4.1 Instance Security

#	QUESTION	SCORE (0-3)	NOTES
33	Are instances using latest/hardened AMIs/images?	_____	
34	Is IMDSv2 enforced (AWS) or equivalent metadata protection?	_____	
35	Are instance profiles/managed identities used (not access keys)?	_____	
36	Is there a patch management process for cloud instances?	_____	

#	QUESTION	SCORE (0-3)	NOTES
37	Are container images scanned for vulnerabilities?	_____	ECR, ACR, GCR scanning
38	Are containers running as non-root?	_____	
39	Is a private container registry used?	_____	

Subsection Score: _____ / 9

4.3 Serverless Security

#	QUESTION	SCORE (0-3)	NOTES
40	Are Lambda/Functions using least privilege IAM roles?	_____	

Subsection Score: _____ / 3

COMPUTE TOTAL: _____ / 24

SECTION 5: MONITORING & LOGGING (8 Questions)

5.1 Cloud Logging

#	QUESTION	SCORE (0-3)	NOTES
41	Is cloud trail/activity logging enabled?	_____	CloudTrail, Azure Activity Log, GCP Audit Logs
42	Are logs sent to a centralized location?	_____	
43	Is log integrity protection enabled?	_____	
44	Are logs retained for at least 1 year?	_____	

Subsection Score: _____ / 12

5.2 Security Monitoring

#	QUESTION	SCORE (0-3)	NOTES
45	Is a cloud security tool (CSPM) deployed?	_____	SecurityHub, Defender, SCC
46	Are security findings reviewed regularly?	_____	
47	Is threat detection enabled?	_____	GuardDuty, Defender, SCC
48	Are alerts configured for critical security events?	_____	

Subsection Score: _____ / 12

MONITORING TOTAL: _____ / 24

6.1 Governance

#	QUESTION	SCORE (0-3)	NOTES
49	Is there a cloud security policy?	_____	
50	Is infrastructure as code (IaC) security scanning in place?	_____	
51	Are tagging standards enforced?	_____	

Subsection Score: _____ / 9

6.2 Compliance

#	QUESTION	SCORE (0-3)	NOTES
52	Is compliance status monitored continuously?	_____	
53	Are compliance reports generated regularly?	_____	
54	Is there a process for remediating compliance violations?	_____	
55	Are cloud provider compliance certifications (SOC 2, etc.) reviewed?	_____	

Subsection Score: _____ / 12

COMPLIANCE TOTAL: _____ / 21

SCORING SUMMARY

Your Cloud Security Scores

SECTION	YOUR SCORE	MAX SCORE	%	RISK LEVEL
Identity & Access	_____	36	___%	_____
Network Security	_____	30	___%	_____
Data Protection	_____	30	___%	_____
Compute Security	_____	24	___%	_____
Monitoring & Logging	_____	24	___%	_____
Compliance & Governance	_____	21	___%	_____
TOTAL	**_____**	**165**	**___%**	_____

 | 4701 Sangamore Road, Suite 100N #2000, Bethesda, MD 20816
hello@platops.com | (202) 864-1197 | platops.com

SCORE %	RISK LEVEL	MISCONFIGURATION RISK
0-25%	**Critical**	High likelihood of breach
26-50%	**High**	Significant exposure
51-75%	**Medium**	Some gaps to address
76-90%	**Low**	Minor improvements needed
91-100%	**Minimal**	Well-secured environment

CRITICAL FINDINGS

Immediate Action Required (Score = 0)

#	FINDING	RISK	REMEDIATION
		Critical / High	
		Critical / High	
		Critical / High	
		Critical / High	

High Priority (Score = 1)

#	FINDING	RISK	REMEDIATION
		High / Medium	
		High / Medium	
		High / Medium	

CLOUD RESOURCE INVENTORY

Critical Resources to Review

RESOURCE TYPE	COUNT	PUBLIC?	ENCRYPTED?
Storage Buckets/Blobs	_____	Y / N	Y / N
Databases (RDS/SQL)	_____	Y / N	Y / N
Compute Instances	_____	-	-
Load Balancers	_____	Y / N	-
API Gateways	_____	Y / N	-

Ready to Secure Your Cloud Environment?

Step 1: Schedule a cloud security consultation → platops.com/book-call

Step 2: Get a professional cloud security assessment → platops.com/assessment

Step 3: Remediate with expert guidance

PlatOps Cloud Security Services

- **Cloud Security Assessment** - Deep-dive evaluation
- **CSPM Implementation** - Continuous monitoring
- **Cloud Hardening** - Configuration remediation
- **Well-Architected Review** - Best practices alignment
- **Managed Cloud Security** - Ongoing protection

Ready to Get Started?

Let our team of security and infrastructure experts help you achieve your goals faster.

100%	60+	8-12 wk	24/7
AUDIT PASS RATE	ORGANIZATIONS SERVED	AVG. TIME TO COMPLIANCE	MONITORING & SUPPORT

Get Free Assessment | Book Strategy Call | Cloud Security Services

Email: hello@platops.com Phone: (202) 864-1197 Web: platops.com