AccuKnox®

Cloud Compliance Report

Report generated on **Feb 12, 2025 12:00:00 (IST)**

Prepared for

Acme Corp

Prepared by

AccuKnox

support@accuknox.com

About the Report

This report provides a detailed evaluation of the organization's compliance posture against applicable regulatory standards and frameworks. It identifies areas of non-compliance, highlights gaps in policies and controls, and offers actionable recommendations to address these issues. The assessment leverages industry best practices and automated compliance validation tools to ensure accuracy and completeness. This report aims to help the organization reduce compliance risk, maintain regulatory adherence, and strengthen governance practices.

Confidentiality Notice

This document contains confidential and proprietary information intended solely for the use of [Company Name]'s executive leadership. Unauthorized disclosure, copying, or distribution of this report is strictly prohibited.

Overall Compliance Summary

last scanned on **Feb 12, 2025 12:00:00**

Cloud Compliance Summary

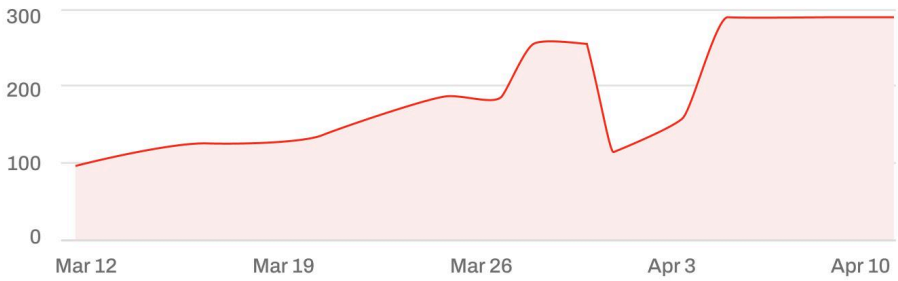
Latest Score

65% ↓ 10%

Checks

903 Checks Passed

1.1k Checks Failed



Manage multiple cloud accounts effortlessly with real-time visibility. Quickly identify active and inactive accounts for better control and governance.

Top 10 Non-Compliant Asset Categories by Severity

Category	Checks								Severity	
Container	120	20	C	10	H	60	M	60	L
AWS Identity	8	2	C	1	H	3	M	2	L
ML Serverless Endpoint	10	7	C	1	H	1	M	1	L
Database	8	8	C	0	H	0	M	0	L
Storage	8	8	C	0	H	0	M	0	L
Host	120	20	C	10	H	60	M	60	L
Workload	8	2	C	1	H	3	M	2	L
Networking	10	7	C	1	H	1	M	1	L
Configuration	8	8	C	0	H	0	M	0	L
Security & Identity	8	8	C	0	H	0	M	0	L

View total cloud assets at a glance with clear insight into impacted assets. Easily track assets affected by security findings for faster risk mitigation.

Compliance Summary by Framework

Framework		Score
AWS CIS Benchmark 1.2.1	↑ 5%	55%
AWS CIS Benchmark 1.2.4	↓ 12%	75%
GCP CIS Benchmark 1.2.1	↑ 5%	95%
NIST 1.2.2	↑ 5%	95%
ISO 27001	↑ 5%	95%

Manage multiple cloud accounts effortlessly with real-time visibility. Quickly identify active and inactive accounts for better control and governance.

Overall Compliance Summary

last scanned on **Feb 12, 2025 12:00:00**

Top 10 Failing Checks

Checks	Severity	Assets
8.4.1 Key Vault Recovery Enabled	Critical	223
8.5.1 Kubernetes RBAC Enabled	Critical	2
1.1.1 Auto Provisioning Enabled	Critical	23
2.1.1 Monitor Disk Encryption	High	14
2.1.3 Security Contacts Enabled	High	56
8.4.1 Key Vault Recovery Enabled	High	444
8.5.1 Kubernetes RBAC Enabled	Medium	10
1.1.1 Auto Provisioning Enabled	Medium	78
2.1.1 Monitor Disk Encryption	Low	15
2.1.3 Security Contacts Enabled	Low	11

View total cloud assets at a glance with clear insight into impacted assets. Easily track assets affected by security findings for faster risk mitigation.

Assets Summary

last scanned on **Feb 12, 2025 12:00:00**

Assets Summary

7,751 Total Assets

2,145 Passed 1,830 Failed 2,540 Warning 1,236 Unknown

Manage multiple cloud accounts effortlessly with real-time visibility. Quickly identify active and inactive accounts for better control and governance.

Top 10 Asset Categories with Failed Checks

Category	Failed Assets
Container	54 / 54 (100%)
AWS Identity	420 / 700 (60%)
ML Serverless Endpoint	1039 / 2100 (49%)
Database	85 / 190 (45%)
Storage	1250 / 3000 (41.7%)
Host	320 / 850 (37.6%)
Workload	150 / 480 (31.3%)
Networking	900 / 3000 (30%)
Configuration	250 / 1000 (25%)
Security & Identity	48 / 250 (19.2%)

View total cloud assets at a glance with clear insight into impacted assets. Easily track assets affected by security findings for faster risk mitigation.

Compliance-Specific Summary

last scanned on **Feb 12, 2025 12:00:00**

This section shows data specific to chosen compliance framework **AWS CIS Benchmark 1.2.1** for the selected cloud asset **956994857092 | AWS.**

AWS CIS Benchmark 1.2.1

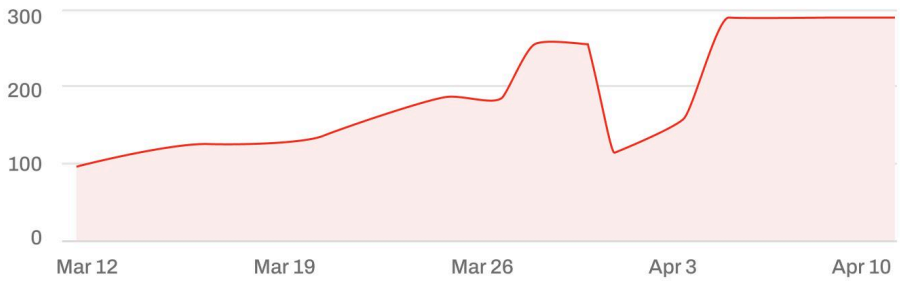
Latest Score

65% ↓ 10%

Checks

903 Checks Passed

1.1k Checks Failed



Manage multiple cloud accounts effortlessly with real-time visibility. Quickly identify active and inactive accounts for better control and governance.

Top 10 Non-Compliant Asset Categories by Severity

Category	Checks								Severity
Container	120	20	C	10	H	60	M	60	L
AWS Identity	8	2	C	1	H	3	M	2	L
ML Serverless Endpoint	10	7	C	1	H	1	M	1	L
Database	8	8	C	0	H	0	M	0	L
Storage	8	8	C	0	H	0	M	0	L
Host	120	20	C	10	H	60	M	60	L
Workload	8	2	C	1	H	3	M	2	L
Networking	10	7	C	1	H	1	M	1	L
Configuration	8	8	C	0	H	0	M	0	L
Security & Identity	8	8	C	0	H	0	M	0	L

View total cloud assets at a glance with clear insight into impacted assets. Easily track assets affected by security findings for faster risk mitigation.

Compliance-Specific Summary

last scanned on **Feb 12, 2025 12:00:00**

Top 10 Failing Checks

Checks	Severity	Assets
8.4.1 Key Vault Recovery Enabled	Critical	223
8.5.1 Kubernetes RBAC Enabled	Critical	2
1.1.1 Auto Provisioning Enabled	Critical	23
2.1.1 Monitor Disk Encryption	High	14
2.1.3 Security Contacts Enabled	High	56
8.4.1 Key Vault Recovery Enabled	High	444
8.5.1 Kubernetes RBAC Enabled	Medium	10
1.1.1 Auto Provisioning Enabled	Medium	78
2.1.1 Monitor Disk Encryption	Low	15
2.1.3 Security Contacts Enabled	Low	11

View total cloud assets at a glance with clear insight into impacted assets. Easily track assets affected by security findings for faster risk mitigation.

Compliance-Specific Summary

last scanned on **Feb 12, 2025 12:00:00**

Compliance Summary

Checks	Asset Category	Type	Assets Status
1.1 Ensures Storage bucket policies do not allow golbal write, delete or read permissions			2/4 checks passed
C Storage bucket all users policy	Storage	M Manual	150 50 50 50
C Bucket Uniform Level Access	Storage	M Manual	150 50 50 50
H MySQL Local Infile Disabled	Database	A Auto	150 50 50 50
H PostgreSQL Log Checkpoints Enabled	Database	A Auto	150 50 50 50
1.2 Ensure that log_checkpoints flag is enabled for PostgreSQL Instances			2/2 checks passed
C PostgreSQL Log Checkpoints Enabled	SQL Configuration Log	M Manual	150 50 50 50
H PostgreSQL Log Min Error Statement	SQL Configuration Log	M Manual	150 50 50 50
1.3 Ensure all user service account keys are being managed by Google			3/5 checks passed
C Bucket Uniform Level Access	SQL Configuration Log	M Manual	150 50 50 50
M Storage bucket all users policy	Networking	A Auto	150 50 50 50
M PostgreSQL Log Checkpoints Enabled	Security & Identity	A Auto	150 50 50 50
M PostgreSQL Log Min Error Statement	SQL Configuration Log	M Manual	150 50 50 50
L PostgreSQL Log Checkpoints Enabled	SQL Configuration Log	M Manual	150 50 50 50
1.4 Ensure SQL instances for mySQL type does not have local infile flag enabled			1/2 checks passed
C PostgreSQL Log Checkpoints Enabled	SQL Configuration Log	M Manual	150 50 50 50
H PostgreSQL Log Min Error Statement	SQL Configuration Log	M Manual	150 50 50 50
1.5 Ensure SQL instances for PostgreSQL type have log connections flag enabled			3/4 checks passed
C Bucket Uniform Level Access	SQL Configuration Log	M Manual	150 50 50 50
M Storage bucket all users policy	Networking	A Auto	150 50 50 50
M PostgreSQL Log Checkpoints Enabled	Security & Identity	A Auto	150 50 50 50
H PostgreSQL Log Checkpoints Enabled	SQL Configuration Log	M Manual	150 50 50 50
2.1 Ensure that separation of duties is enforces while assigning service account			9/12 checks passed
C Bucket Uniform Level Access	SQL Configuration Log	M Manual	150 50 50 50
C Storage bucket all users policy	Networking	A Auto	150 50 50 50
C PostgreSQL Log Checkpoints Enabled	Security & Identity	A Auto	150 50 50 50
H PostgreSQL Log Checkpoints Enabled	SQL Configuration Log	M Manual	150 50 50 50
H Bucket Uniform Level Access	SQL Configuration Log	M Manual	150 50 50 50
H Storage bucket all users policy	Networking	A Auto	150 50 50 50
M PostgreSQL Log Checkpoints Enabled	Security & Identity	A Auto	150 50 50 50
M PostgreSQL Log Checkpoints Enabled	SQL Configuration Log	M Manual	150 50 50 50

Compliance-Specific Summary

last scanned on **Feb 12, 2025 12:00:00**

Compliance Summary

Checks	Asset Category	Type	Assets Status			
M Storage bucket all users policy	Storage	M Manual	150	50	50	50
M Bucket Uniform Level Access	Storage	M Manual	150	50	50	50
L MySQL Local Infile Disabled	Database	A Auto	150	50	50	50
L PostgreSQL Log Checkpoints Enabled	Database	A Auto	150	50	50	50
2.2 Ensure that log_checkpoints flag is enabled for PostgreSQL Instances						2/2 checks passed
C PostgreSQL Log Checkpoints Enabled	SQL Configuration Log	M Manual	150	50	50	50
H PostgreSQL Log Min Error Statement	SQL Configuration Log	M Manual	150	50	50	50
3.1 Ensure all user service account keys are being managed by Google						3/5 checks passed
C Bucket Uniform Level Access	SQL Configuration Log	M Manual	150	50	50	50
M Storage bucket all users policy	Networking	A Auto	150	50	50	50
M PostgreSQL Log Checkpoints Enabled	Security & Identity	A Auto	150	50	50	50
M PostgreSQL Log Min Error Statement	SQL Configuration Log	M Manual	150	50	50	50
L PostgreSQL Log Checkpoints Enabled	SQL Configuration Log	M Manual	150	50	50	50

Region Based Findings

Region	Count			Status
us-east-1	140	10	60	60
us-west-2	155	25	44	32
mumbaicentral	234	89	90	12
india-south-2	100	15	15	55
ap-southeast-1	56	8	12	37
eu-west-3	110	100	6	0
global	11	10	0	0

View total cloud assets at a glance with clear insight into impacted assets. Easily track assets affected by security findings for faster risk mitigation.

Compliance-Specific Summary

last scanned on **Feb 12, 2025 12:00:00**

Open Tickets for Critical & High Severity Findings

Ticket ID	Finding	Ticket Severity	Age (Days)
1001	CloudTrail global services event logging is not enabled:	Critical	120
1002	IAM Master and Manager Roles not found	Critical	88
1003	Key Vaults are not being used to store secrets	High	64
1004	Maximum password reuse of: 1 passwords is less than 5	High	12
1005	Network Watcher is not enabled in the region	High	9

Automatically open tickets for critical and high-severity findings to ensure prompt action. Streamline incident management by prioritizing high-impact issues with clear, actionable tickets.

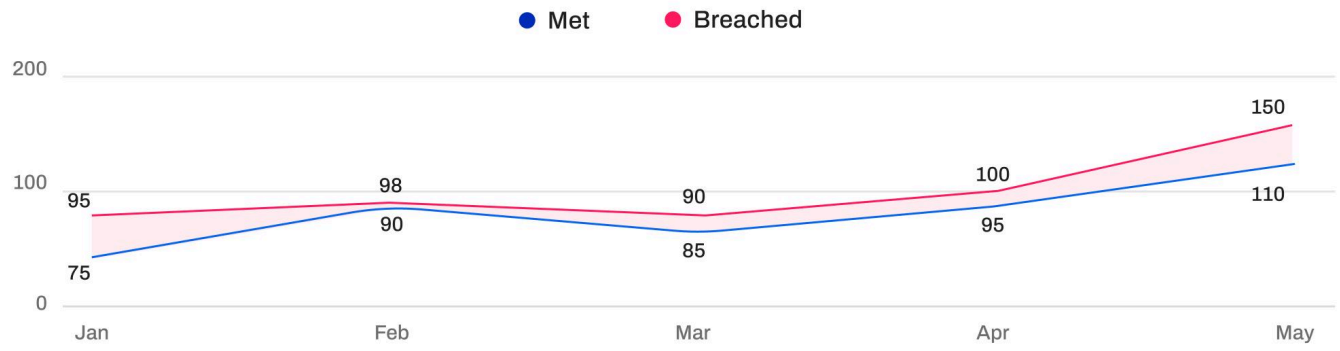
SLA Status

660 Open Tickets

Status	Total	Severity			
Breached	200	100 C	75 H	15 M	10 L
At Risk	450	350 C	50 H	25 M	25 L
Within SLA	10	3 C	2 H	5 M	5 L

Track the SLA status of tickets to ensure timely resolution and compliance. Easily identify tickets approaching their SLA deadline or those that have breached the SLA for faster intervention.

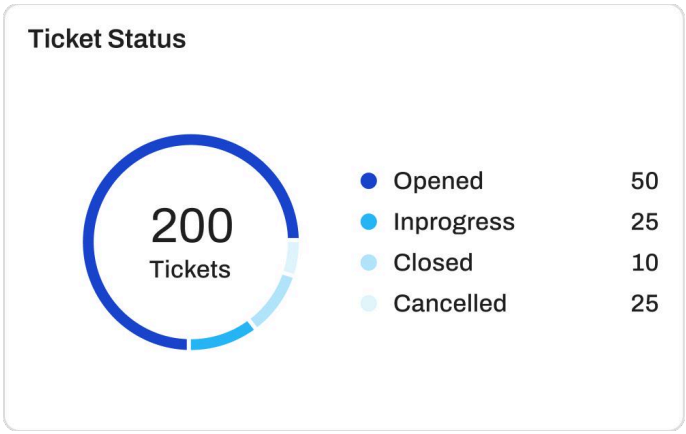
Tickets Resolution Trend



Visualize ticket resolution trends over time with counts of SLA met vs. breached. Identify performance patterns and optimize response efforts across teams.

Compliance-Specific Summary

last scanned on **Feb 12, 2025 12:00:00**



Track support or remediation progress with a snapshot of ticket statuses. Quickly view open, in-progress, and resolved tickets to stay on top of issues.