NuboLabs

NuboComply

Multi-Framework Compliance Audit

🔴 Poor

Acme Technologies Ltd	15 May 2026	772147490302	EU-WEST-2	147	6
Client	Date	AWS Account	Region	Findings	Critical

Executive Summary

What you need to know before reading anything else.

26	6	5	1	32
Score / 100	Critical	High	Medium	Passing

Acme Technologies Ltd's NuboComply audit reveals a score of **26/100**. With 6 critical and 5 high findings, immediate action is required. The priority actions below will have the greatest impact.

⚠ **If you fix nothing:** You will fail your next SOC2 or ISO27001 audit. Enterprise clients will reject vendor questionnaires. GDPR technical measures unmet.

Top 5 Priority Actions

Start here. Highest impact on your score and risk posture.

1 **Root account MFA enabled** — CRITICAL

AWS master account has no second factor. Anyone with the password has complete control.

→ Enable MFA on root account immediately — use hardware MFA key

2 **Port 22 (SSH) not open to 0.0.0.0/0** — CRITICAL

This finding requires immediate attention. Review the affected resource and apply the recommended fix below.

→ Restrict SSH to specific IPs or use SSM Session Manager instead

3 **Port 3389 (RDP) not open to 0.0.0.0/0** — CRITICAL

This finding requires immediate attention. Review the affected resource and apply the recommended fix below.

→ Restrict RDP to specific IPs — use VPN or bastion host

4 **CloudTrail enabled and logging** — CRITICAL

No audit trail. A breach would be completely untraceable.

→ Enable CloudTrail with multi-region logging immediately

5 **No secrets in Lambda environment variables** — CRITICAL

This finding requires immediate attention. Review the affected resource and apply the recommended fix below.

→ Move all secrets to Secrets Manager — use SDK to fetch at runtime

Framework Readiness Scorecard

Technical control coverage across all 9 compliance frameworks.

FRAMEWORK	PASS	FAIL	SCORE	%
SOC2 Type II	38	109		26%
ISO 27001:2022	38	109		26%
CIS AWS v2.0	44	103		30%
GDPR Art.32	38	109		26%
UK Cyber Essentials	85	62		58%
NCSC CSP	37	110		25%
NIST CSF 2.0	38	109		26%
PCI DSS v4.0	40	107		27%
AWS Well-Architected	38	109		26%

Attack Path Analysis

How an attacker exploits your specific findings — step by step.

⚠ How an attacker exploits these findings

1. **Root account MFA enabled**
   AWS master account has no second factor. Anyone with the password has complete control.

↓

2. **Port 22 (SSH) not open to 0.0.0.0/0**
   Port 22 open to the internet — attackers scan for this within minutes.

↓

3. **Port 3389 (RDP) not open to 0.0.0.0/0**
   Port 3389 open to the internet — primary ransomware entry point.

↓

4. **CloudTrail enabled and logging**
   No audit trail. A breach would be completely untraceable.

✓ **Fix any one step above and you break the entire attack chain.**

Critical Findings (6)

Immediate action required.

CRITICAL

IAM-1.2: Root account MFA enabled

What it means The AWS root account is the master account created when you first signed up for AWS. It has unrestricted access to every service and resource, cannot be restricted by IAM policies, and if compromised gives an attacker complete and permanent control over your entire AWS environment.

How to fix Enable MFA via IAM Console → Security credentials → Multi-factor authentication. Use a hardware MFA key (YubiKey) or authenticator app (Google Authenticator, Authy). After enabling, the root account should never be used for day-to-day operations.

Positive impact Closes the single most critical attack vector in AWS. Even if the root password is compromised, the attacker cannot access the account without the second factor. Required by SOC2, ISO27001, CIS AWS Benchmark, and PCI DSS.

Considerations If you lose the MFA device without backup codes, account recovery requires contacting AWS support with identity verification — can take days. Mitigation: store backup codes securely.

Effort Very low — 10 minutes. Highest priority action in any AWS account.

`SOC2:CC6.1 · ISO27001:A.8.5 · CIS:1.5 · GDPR:Art32(1)(b) · PCI:Req8.4`

CRITICAL

NET-2.1: Port 22 (SSH) not open to 0.0.0.0/0

What it means Port 22 (SSH) is open to 0.0.0.0/0 — meaning any computer on the internet can attempt to connect to your EC2 instances. Automated bots scan the entire internet for open SSH ports continuously. Within hours of an instance launching, it will receive thousands of login attempts.

How to fix Restrict the security group rule to your office IP or VPN CIDR range. Better: remove SSH access entirely and use AWS Systems Manager Session Manager — provides encrypted shell access with full audit logging, no port 22 required, no key management.

Positive impact Eliminates the most common initial access vector for EC2 compromises. Session Manager provides better security AND better audit trail than SSH. Required by CIS AWS Benchmark 5.1.

Considerations Restricting to a specific IP breaks access if working remotely. Session Manager requires SSM agent installed (included in Amazon Linux 2+, Ubuntu 20.04+). Slightly more complex initial setup.

Effort Low — 15 minutes to restrict to VPN/office IP. Medium to fully migrate to Session Manager.

`SOC2:CC6.6 · ISO27001:A.8.20 · CIS:5.1 · GDPR:Art32(1)(b) · PCI:Req1.3`

CRITICAL

NET-2.2: Port 3389 (RDP) not open to 0.0.0.0/0

What it means Port 3389 (RDP - Remote Desktop Protocol) is open to 0.0.0.0/0 — any computer on the internet can attempt to connect. RDP is the primary attack vector for ransomware groups. It is scanned for continuously by automated bots and criminal groups who sell RDP access on dark web markets.

How to fix Restrict the security group inbound rule to your office/VPN IP range only. Better: disable RDP entirely and use AWS Systems Manager Session Manager for remote access — no port required, full audit logging, encrypted.

Positive impact Eliminates the #1 ransomware entry point. RDP brute force is responsible for 50%+ of ransomware incidents. Required by CIS AWS Benchmark 5.2, SOC2 CC6.6, PCI DSS Req1.3.

Considerations Restricting to a specific IP breaks access when working from different locations. Requires VPN or Session Manager setup for remote access.

Effort Low — 10 minutes to restrict. Medium to migrate to Session Manager.

`SOC2:CC6.6 · ISO27001:A.8.20 · CIS:5.2 · GDPR:Art32(1)(b) · PCI:Req1.3`

CRITICAL

LOG-4.1: CloudTrail enabled and logging

What it means AWS CloudTrail records every API call made in your AWS account — who did what, when, from where. Without it, there is zero visibility into what actions have been taken. If your account is breached, you cannot determine what the attacker accessed, modified, or deleted. You also cannot prove compliance to any auditor.

How to fix Enable via CloudTrail Console → Create trail. Enable for all regions, enable log file validation, store logs in S3 with versioning enabled. Cost: approximately £1-3/month for a typical account.

Positive impact Complete audit trail for security investigations and compliance. Required by SOC2 CC7.1, ISO27001 A.8.15, CIS 3.1, GDPR Art.32(1)(d), PCI DSS Req10.1. Enables incident response and forensic investigation.

Considerations Small ongoing cost (£1-3/month). Log volume can be high in large accounts. Without a SIEM, raw CloudTrail logs are difficult to query.

Effort Very low — 10 minutes to enable.

`SOC2:CC7.1 · ISO27001:A.8.15 · CIS:3.1 · GDPR:Art32(1)(d) · PCI:Req10.1`

CRITICAL

SEC-6.1: No secrets in Lambda environment variables

What it means Lambda functions with exposed secrets: nubocomply-demo-api, nubocomply-demo-worker

How to fix: Move all secrets to Secrets Manager — use SDK to fetch at runtime

`SOC2:C1.2 · ISO27001:A.8.11 · GDPR:Art32(1)(a) · PCI:Req3.4`

CRITICAL

AVL-5.1: RDS automated backups enabled

What it means If database fails, data is permanently lost.

Detail DBs without backups: nubocomply-demo-db

How to fix: Enable automated backups with minimum 7-day retention

`SOC2:A1.3 · ISO27001:A.8.13 · CIS:2.9 · GDPR:Art32(1)(c) · PCI:Req3.1`

High Findings (5)

Address within 48 hours.

HIGH

IAM-1.3: IAM password policy meets requirements

What it means Policy issues: min length < 14, no complexity requirements

How to fix: Set: min 14 chars, require symbols/numbers/upper/lower, 90-day max age

SOC2:CC6.1 · ISO27001:A.8.5 · CIS:1.8 · PCI:Req8.3

HIGH

IAM-1.4: All IAM console users have MFA enabled

What it means Multi-factor authentication (MFA) requires users to provide a second form of verification (a time-based one-time code) in addition to their password. Without MFA, a single compromised password gives an attacker immediate full access to the account.

How to fix Enable per-user via IAM Console → Users → Security credentials → Assign MFA device. Enforce via IAM policy that denies all actions if MFA is not present. Use authenticator apps (Google Authenticator, Authy) or hardware keys (YubiKey).

Positive impact Eliminates credential theft as an attack vector. Required by SOC2, ISO27001, PCI DSS, and CIS Benchmark. Reduces cyber insurance premiums. Simple to implement.

Considerations Users must have their phone or hardware key available to log in. Loss of MFA device requires admin intervention to recover access.

Effort Low — 10-15 minutes per user.

SOC2:CC6.1 · ISO27001:A.8.5 · CIS:1.12 · PCI:Req8.4

HIGH

NET-2.6: VPC flow logs enabled

What it means VPCs without flow logs: vpc-062e6f0e9f4f0ceae

How to fix: Enable VPC flow logs to CloudWatch Logs or S3

SOC2:CC7.1 · ISO27001:A.8.15 · CIS:3.9 · GDPR:Art32(1)(d)

HIGH

NET-2.8: All EBS volumes encrypted at rest

What it means 6 unencrypted volumes found

How to fix: Encrypt via: snapshot → copy with encryption → restore

SOC2:CC6.7 · ISO27001:A.8.24 · CIS:2.6 · GDPR:Art32(1)(a)

HIGH

RDS-3.9: All RDS instances encrypted at rest

What it means Unencrypted DBs: nubocomply-demo-db

How to fix: Encrypt via: snapshot → copy with encryption enabled → restore

SOC2:CC6.7 · ISO27001:A.8.24 · CIS:2.7 · GDPR:Art32(1)(a)

Medium Findings (1)

Address within 2 weeks.

MEDIUM

LOG-4.8: CloudWatch log groups have retention policies

What it means 12 log groups without retention policies

How to fix: Set 90-day retention on app logs, 1-year on audit logs

SOC2:CC7.1 · ISO27001:A.5.33 · GDPR:Art5(1)(e)

Manual Verification Required

3 controls require human verification.

✎ **GOV-9.1: Information security policy documented and approved**

Information security policy signed by management and reviewed annually

✎ **AVL-5.8: Business continuity plan documented and tested**

Document BCP with RTO/RPO targets and test recovery procedures annually

✎ **AVL-5.9: Incident response plan documented and tested**

Document incident response procedures — detection, containment, recovery

Remediation Roadmap

Prioritised fix order — hand this to your engineering team.

1	**Root account MFA enabled** Enable MFA on root account immediately — use hardware MFA key	CRITICAL	30 min
2	**Port 22 (SSH) not open to 0.0.0.0/0** Restrict SSH to specific IPs or use SSM Session Manager instead	CRITICAL	30 min
3	**Port 3389 (RDP) not open to 0.0.0.0/0** Restrict RDP to specific IPs — use VPN or bastion host	CRITICAL	30 min
4	**CloudTrail enabled and logging** Enable CloudTrail with multi-region logging immediately	CRITICAL	30 min
5	**No secrets in Lambda environment variables** Move all secrets to Secrets Manager — use SDK to fetch at runtime	CRITICAL	30 min
6	**RDS automated backups enabled** Enable automated backups with minimum 7-day retention	CRITICAL	30 min
7	**IAM password policy meets requirements** Set: min 14 chars, require symbols/numbers/upper/lower, 90-day max age	HIGH	2–4 hrs
8	**All IAM console users have MFA enabled** Enable MFA for all IAM users with console access	HIGH	2–4 hrs
9	**VPC flow logs enabled** Enable VPC flow logs to CloudWatch Logs or S3	HIGH	2–4 hrs
10	**All EBS volumes encrypted at rest** Encrypt via: snapshot → copy with encryption → restore	HIGH	2–4 hrs
11	**All RDS instances encrypted at rest** Encrypt via: snapshot → copy with encryption enabled → restore	HIGH	2–4 hrs
12	**CloudWatch log groups have retention policies** Set 90-day retention on app logs, 1-year on audit logs	MEDIUM	1 day

Need help fixing these?

NuboLabs offers full remediation — we implement the fixes for you.

Targeted Fix

We remediate the critical and high findings from this report. Done properly by the same engineer who found them.

From £500

Full Hardening

Complete implementation of all findings plus architectural improvements. Leaves your environment in a production-ready secure state.

From £1,500

POPULAR

Monthly Retainer

Monthly rescan plus ongoing remediation as your infrastructure evolves. New findings fixed before they become incidents.

From £600/mo

Ready to get started?

Reply to this report or get in touch directly.

sales@nubolabs.co.uk

nubolabs.co.uk · Leeds, UK

NuboLabs

Cloud Infrastructure Intelligence

kenziebollon@nubolabs.co.uk

nubolabs.co.uk · Leeds, UK