

# Cloud:TbV

---

## Executive Risk Report

Acme SaaS Ltd

Account: \*\*\*\*-\*\*\*\*-7823

April 2026

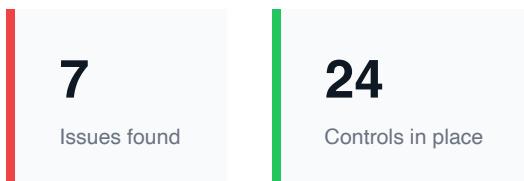
Report date: 19 April 2026

Framework: CIS AWS Foundations Benchmark v2.0, SOC 2

OVERALL RISK

# HIGH

▲ 1 fewer issue than last month



---

This report does not guarantee audit outcomes, regulatory compliance, or the absence of security vulnerabilities.

## Security Posture

---

Your AWS environment was scanned against the CIS AWS Foundations Benchmark v2.0, SOC 2. 7 issues were identified that require attention.

**3** High

**4** Medium

▲ 1 fewer issue than last month

## Issues Requiring Attention

---

The following issues are listed in order of risk. Each represents a real exposure to your business or data.

**HIGH** eu-west-1

Server management ports are open to the entire internet — infrastructure is exposed to automated brute-force and credential-stuffing attacks.

**Action:** Restrict SSH (port 22) inbound rules to specific trusted IP ranges.

**HIGH** eu-west-1

Console users without MFA are one stolen password away from a full account compromise — phishing attacks become immediately effective.

**Action:** Enable MFA for all IAM users with console access in IAM → Users → Security credentials.

**HIGH** eu-west-1

New EC2 storage volumes are created unencrypted by default — sensitive data written to disk is not protected at rest.

**Action:** Enable EBS encryption by default in EC2 → Settings → EBS encryption.

**MEDIUM** eu-west-1

Unused credentials remain active — former employees or compromised accounts could silently access systems without detection.

**Action:** Disable or remove credentials unused for 90+ days in IAM Users.

**MEDIUM** eu-west-1

Long-lived access keys increase the window of exposure if a key is leaked — stale keys in old repositories become persistent risks.

**Action:** Rotate access keys older than 90 days and update any systems using them.

**MEDIUM** eu-west-1

Default network firewall rules are overly permissive — new AWS resources may automatically inherit unsafe network access.

**Action:** Remove all inbound and outbound rules from the default security group.

**MEDIUM** eu-west-1

EC2 instances accept unauthenticated metadata requests — a server-side request forgery (SSRF) flaw could allow attackers to steal IAM credentials.

**Action:** Enforce IMDSv2 on all EC2 instances by setting HttpTokens to 'required' in instance metadata options.

## Compliance Progress

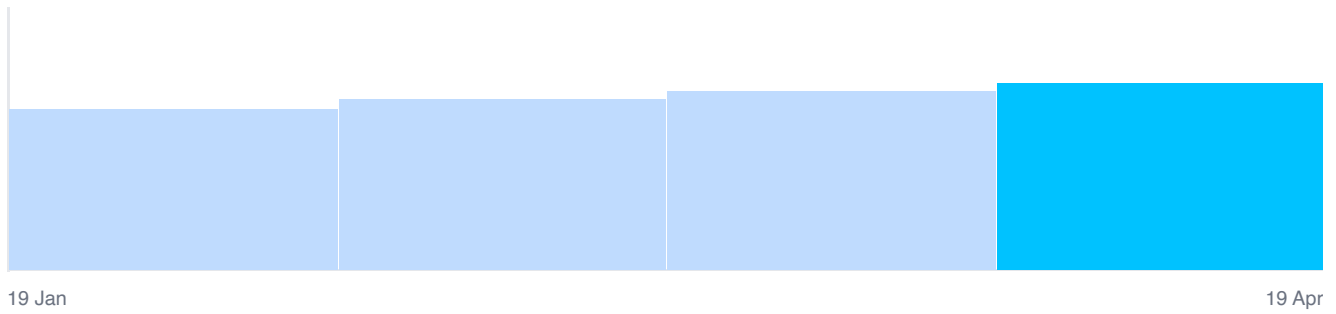
---

Your compliance score measures the percentage of security controls passing across all scanned regions. Higher is better.

# 71%

Current compliance score

Up 10 points over this period



## What's Protected

---

The following controls are in place and working correctly across your environment.

- ✓ No permanent master account credentials are exposed

---

- ✓ Master account is protected with multi-factor authentication

---

- ✓ Remote desktop ports are not exposed to the internet

---

- ✓ No database instances are exposed to the public internet

---

- ✓ Audit log storage is protected from public access

---

- ✓ All database instances have storage encryption enabled

---

- ✓ Access permissions are centrally managed through groups and roles

---

- ✓ All storage is protected from public internet access

---

- ✓ All data transfers to storage are enforced to use encryption

---

- ✓ IAM password policy enforces a strong minimum length

---

- ✓ IAM password policy prevents reuse of recent passwords

---

- ✓ All IAM users operate with a single active access key

---

- ✓ All shared file systems are encrypted at rest

---

- ✓ S3 versioned objects are protected with MFA Delete

---

- ✓ A full audit trail of account activity is being recorded

---

- ✓ Audit logs are tamper-proof and verifiable

---

- ✓ Security events are forwarded to real-time monitoring

---

- ✓ Access to audit log storage is fully tracked

---

- ✓ Network traffic is logged across all VPCs

---

- ✓ AWS Config is recording all resource configuration changes

---

- ✓ Audit logs are encrypted with a customer-managed key

---

- ✓ All customer-managed encryption keys are automatically rotated

---

- ✓ A dedicated support role is available for AWS Support interactions

---

- ✓ IAM Access Analyzer is monitoring for unintended external access

## SOC 2 Criteria Coverage

The following shows how your current AWS security posture maps to SOC 2 Trust Services Criteria. This is intended to support your audit preparation — it does not constitute a formal SOC 2 assessment.

4

Criteria met

3

Criteria at risk

### CC6.1 Logical Access Controls

AT RISK

Console users without MFA are one stolen password away from a full account compromise — phishing attacks become immediately effective.

New EC2 storage volumes are created unencrypted by default — sensitive data written to disk is not protected at rest.

### CC6.2 Credential Management

AT RISK

Unused credentials remain active — former employees or compromised accounts could silently access systems without detection.

Console users without MFA are one stolen password away from a full account compromise — phishing attacks become immediately effective.

Long-lived access keys increase the window of exposure if a key is leaked — stale keys in old repositories become persistent risks.

### CC6.3 Role-based Access Management

MET

### CC6.6 Security Threats and Vulnerabilities

AT RISK

Server management ports are open to the entire internet — infrastructure is exposed to automated brute-force and credential-stuffing attacks.

Default network firewall rules are overly permissive — new AWS resources may automatically inherit unsafe network access.

EC2 instances accept unauthenticated metadata requests — a server-side request forgery (SSRF) flaw could allow attackers to steal IAM credentials.

### CC6.7 Transmission Protection

MET

### CC7.2 System Monitoring

MET

### CC7.3 Security Event Evaluation

MET