SOC 2 READINESS REPORT

Acme Corp

DATE	ENVIRONMENT	REGIONS
May 14, 2026	AWS · [REDACTED]	us-east-1 · us-west-2

SOC 2 READINESS SCORE

72

↓ -4 vs last month

AI RISK SCORE

78

4 AI/agentic findings

CRITICAL FINDINGS

2

Require immediate action

Executive Summary

SOC 2 READINESS SCORE

72

↓ -4 vs last month · Regression in CC7

AI RISK SCORE

78

4 AI/agentic findings · 1 critical

2	4	4	1	10
Critical Findings	High Findings	Medium Findings	Critical AI Risk	Total Open Findings

CHANGES SINCE LAST REPORT

12 New gaps identified	5 Findings resolved	0 Regressions

CONTROL FAMILY STATUS

CONTROL FAMILY	CHECKS	PASSING	FAILING	CRITICAL	COVERAGE
AI_RISK AI & Agentic Risk	4	0	4	1	0%
CC6 Logical Access Controls	5	2	3	1	40%
CC7 System Operations	5	1	4	—	20%
CC8 Change Management	2	1	1	—	50%

AI & Agentic Tool Risk

FLINTWOOD EXCLUSIVE

⚠ **Immediate attention required.** 1 critical and 2 high AI risk findings require remediation. These findings represent gaps in AI governance that could affect your SOC 2 audit posture and introduce real security risk from autonomous or over-permissioned AI workloads.

CRITICAL AI RISK **Over-permissioned Bedrock agent role** AI_RISK.1

`arn:aws:iam::[REDACTED]:role/bedrock-agent-prod`

REMEDIATION

Scope `bedrock:InvokeModel` to specific model ARNs. Remove S3 write permissions or add explicit MFA condition.

HIGH AI RISK **Bedrock invocation logging disabled** AI_RISK.2

`arn:aws:bedrock:us-east-1:[REDACTED]:logging-config`

REMEDIATION

Enable Bedrock model invocation logging to S3 or CloudWatch. Configure 90-day retention.

HIGH AI RISK **Autonomous Lambda chain without approval gate** AI_RISK.3

`arn:aws:lambda:us-east-1:[REDACTED]:function/ai-processor`

REMEDIATION

Implement a human approval step via Step Functions before write operations.

MEDIUM AI RISK **Shadow AI workloads detected** AI_RISK.4

`arn:aws:iam::[REDACTED]:role/*`

REMEDIATION

Tag all AI workloads and audit untagged Bedrock callers.

Critical & High Findings

CRITICAL 2 findings

CRITICAL AI Over-permissioned Bedrock agent role — AI_RISK.1

`arn:aws:iam::[REDACTED]:role/bedrock-agent-prod`

REMEDIATION

Scope `bedrock:InvokeModel` to specific model ARNs. Remove S3 write permissions or add explicit MFA condition.

CRITICAL Root account access keys active — CC6.3

`arn:aws:iam::[REDACTED]:root`

REMEDIATION

Delete root access keys immediately via IAM console.

HIGH 4 findings

HIGH AI Bedrock invocation logging disabled — AI_RISK.2

`arn:aws:bedrock:us-east-1:[REDACTED]:logging-config`

REMEDIATION

Enable Bedrock model invocation logging to S3 or CloudWatch. Configure 90-day retention.

HIGH AI Autonomous Lambda chain without approval gate — AI_RISK.3

`arn:aws:lambda:us-east-1:[REDACTED]:function/ai-processor`

REMEDIATION

Implement a human approval step via Step Functions before write operations.

HIGH IAM users without MFA — CC6.2

`arn:aws:iam::[REDACTED]:user/*`

REMEDIATION

Enforce MFA for all IAM users with console access.

HIGH CloudTrail log validation disabled — CC7.1

`arn:aws:cloudtrail:us-east-1:[REDACTED]:trail/management-trail`

REMEDIATION

Enable log file validation on all CloudTrail trails.

Remediation Roadmap

Prioritized by severity. Address P1 items before your next audit conversation.

P1 — Fix immediately

AI **Over-permissioned Bedrock agent role**
Scope bedrock:InvokeModel to specific model ARNs. Remove S3 write permissions or add explicit MFA condition.

Root account access keys active
Delete root access keys immediately via IAM console.

P2 — Fix within 30 days

AI **Bedrock invocation logging disabled**
Enable Bedrock model invocation logging to S3 or CloudWatch. Configure 90-day retention.

CloudTrail log validation disabled
Enable log file validation on all CloudTrail trails.

IAM users without MFA
Enforce MFA for all IAM users with console access.

AI **Autonomous Lambda chain without approval gate**
Implement a human approval step via Step Functions before write operations.

P3 — Fix within 90 days

S3 buckets missing access logging
Enable S3 server access logging on all buckets containing sensitive data.

AWS Config recorder stopped in us-west-2
Enable AWS Config recorder in all active regions.

AI **Shadow AI workloads detected**
Tag all AI workloads and audit untagged Bedrock callers.

GuardDuty finding: TorIPCaller
Immediately rotate credentials for affected IAM user.

All Findings by Control Family

CC6 — Logical Access Controls

5 checks · 2 passing · 3 failing

CRITICAL ✗ FAIL **Root account access keys active** CC6.3

`arn:aws:iam::[REDACTED]:root`

REMEDIATION

Delete root access keys immediately via IAM console.

HIGH ✗ FAIL **IAM users without MFA** CC6.2

`arn:aws:iam::[REDACTED]:user/*`

REMEDIATION

Enforce MFA for all IAM users with console access.

LOW ✗ FAIL **Password policy: no 90-day rotation** CC6.5

`arn:aws:iam::[REDACTED]:account-summary`

REMEDIATION

Update IAM password policy to require password change every 90 days.

CC7 — System Operations

5 checks · 1 passing · 4 failing

HIGH ✗ FAIL **CloudTrail log validation disabled** CC7.1

`arn:aws:cloudtrail:us-east-1:[REDACTED]:trail/management-trail`

REMEDIATION

Enable log file validation on all CloudTrail trails.

MEDIUM ✗ FAIL **S3 buckets missing access logging** CC7.4

`arn:aws:s3:::acme-customer-data`

REMEDIATION

Enable S3 server access logging on all buckets containing sensitive data.

MEDIUM ✗ FAIL **GuardDuty finding: TorIPCaller** CC7.3

`arn:aws:guardduty:us-east-1:[REDACTED]:detector/abc123`

REMEDIATION

Immediately rotate credentials for affected IAM user.

LOW ✗ FAIL **CloudTrail not delivering to CloudWatch Logs** CC7.2

`arn:aws:cloudtrail:us-east-1:[REDACTED]:trail/management-trail`

REMEDIATION

Configure CloudTrail to deliver logs to CloudWatch Logs.

CC8 — Change Management

2 checks · 1 passing · 1 failing

MEDIUM ✗ FAIL **AWS Config recorder stopped in us-west-2** CC8.2

arn:aws:config:us-west-2:[REDACTED]:configuration-recorder

REMEDIATION

Enable AWS Config recorder in all active regions.