

DEMARKOCLOUD

AWS Cloud Health Check

Cloud Foundation & Architecture Review

Client: BlueRiver Accounting LLC

Environment: AWS - us-east-1

Assessment mode: Read-only review / No production changes

DEMONSTRATION ENVIRONMENT - FICTIONAL CLIENT

64 / 100

ATTENTION REQUIRED

3 High | 3 Medium | 1 Moderate finding

BUILD | AUTOMATE | DEPLOY | SCALE

Executive Summary

DemarkoCloud conducted a read-only assessment of BlueRiver Accounting's AWS environment to evaluate infrastructure health, security and access, operational reliability, backup and recovery preparedness, monitoring, cost-efficiency opportunities, and documentation.

The AWS environment is currently **operational**, and this assessment did not identify evidence requiring DemarkoCloud to characterize the environment as unstable. However, several conditions warrant attention.

Three higher-priority findings involve **privileged access, administrative network exposure, and unvalidated recovery capability**. Additional opportunities involve monitoring coverage, EC2 utilization, application-performance investigation, and architecture documentation.

MOST IMPORTANT CONCLUSION

BlueRiver does not need an immediate AWS redesign. The priority is to **reduce known risk, validate recovery, improve visibility, investigate performance, and then evaluate optimization**.

Cloud Health Score

Assessment Area	Score	Status
Security & Access	55 / 100	Attention Required
Reliability	62 / 100	Improvement Recommended
Backup & Recovery	58 / 100	Attention Required
Monitoring	60 / 100	Improvement Recommended
Cost Efficiency	68 / 100	Review Recommended
Documentation	75 / 100	Moderate
OVERALL	64 / 100	ATTENTION REQUIRED

The score is an executive indicator based on conditions observed during the assessment. It does not mean that 64% of AWS is configured correctly.

Risk Dashboard

Priority	Finding	Summary
HIGH	BR-001	Former administrator access remains enabled.
HIGH	BR-002	SSH is permitted from 0.0.0.0/0 to an application server.
HIGH	BR-003	Backups exist, but recovery has not been validated.

Priority	Finding	Summary
MEDIUM	BR-004	Application performance requires further investigation.
MEDIUM	BR-005	Potential EC2 rightsizing opportunity requires validation.
MEDIUM	BR-006	CloudWatch monitoring coverage is limited.
MODERATE	BR-007	Architecture documentation is outdated.

Detailed Findings

Former Administrator Access

BR-001	HIGH	Identity & Access Management
--------	------	------------------------------

Observation

An IAM user associated with BlueRiver's former AWS consultant remains enabled, retains administrator-level permissions, and has an active access key.

Why this matters

Privileged identities should correspond to legitimate current business requirements. An unused administrator identity unnecessarily increases exposure.

DemarkoCloud recommendation

Determine whether the identity or associated credentials are used by applications, scripts, integrations, or operational processes. Once BlueRiver confirms that no required dependencies exist, remove unnecessary access through its approved access-management process.

Assessment boundary

DemarkoCloud did not disable or delete the identity during this assessment.

Unrestricted SSH Access

BR-002	HIGH	Network Security
--------	------	------------------

Observation

A security group associated with an application server permits inbound SSH on TCP port 22 from **0.0.0.0/0**.

Why this matters

This configuration exposes an administrative service to connection attempts originating from any internet address.

DemarkoCloud recommendation

Determine the legitimate administrative-access requirement and establish an appropriately restricted management path. Potential approaches should be evaluated against BlueRiver's operational requirements before production access is modified.

Assessment boundary

No security-group rules were changed during this assessment.

Recovery Capability Not Validated

BR-003	HIGH	Business Continuity
--------	------	---------------------

Observation

EBS snapshots and RDS automated backups are present, but BlueRiver could not provide evidence of a documented recovery test.

Why this matters

The existence of backup artifacts does not, by itself, demonstrate that critical workloads can be recovered within acceptable business requirements.

DemarkoCloud recommendation

Develop a controlled recovery-validation procedure and test restoration of an appropriate workload. Document recovery steps, responsible personnel, expected recovery time, dependencies, validation criteria, and test results.

Assessment boundary

DemarkoCloud is not stating that the backups are defective; the finding is that recovery capability has not been validated.

Application Performance Requires Further Investigation

BR-004	MEDIUM	Performance & Reliability
--------	--------	---------------------------

Observation

Employees report degraded document-management performance during high-demand periods. Available CPU metrics do not provide sufficient evidence to determine root cause.

Why this matters

Low average CPU utilization does not rule out memory, storage I/O, database, network, application, or concurrency constraints.

DemarkoCloud recommendation

Correlate reported performance periods with EC2 CPU and memory utilization, disk I/O, network activity, application metrics, RDS/database performance, and workload concurrency before proposing a production change.

Assessment boundary

Current conclusion: **root cause undetermined**.

Potential EC2 Rightsizing Opportunity

BR-005	MEDIUM	Cost Optimization
--------	--------	-------------------

Observation

Two EC2 instances demonstrate relatively low average CPU utilization.

Why this matters

The workloads may be candidates for rightsizing, but CPU utilization alone is insufficient to make a safe production sizing decision.

DemarkoCloud recommendation

Review memory, storage I/O, network throughput, workload schedules, application requirements, peak utilization, and operational dependencies before changing instance sizes.

Assessment boundary

No savings amount is promised by this assessment.

Limited Operational Monitoring

BR-006	MEDIUM	Monitoring & Operations
--------	--------	-------------------------

Observation

Only two meaningful CloudWatch alarms were identified despite multiple EC2 instances, an RDS database, and an Application Load Balancer.

Why this matters

Limited alert coverage can delay awareness of infrastructure degradation or failure, particularly when the organization does not have dedicated AWS operations staff.

DemarkoCloud recommendation

Define monitoring requirements for business-critical infrastructure and establish appropriate alerts for application availability, infrastructure health, database health, resource utilization, and failure conditions.

Architecture Documentation Is Outdated

BR-007	MODERATE	Documentation
--------	----------	---------------

Observation

BlueRiver's architecture diagram shows three EC2 instances and does not accurately represent the current Application Load Balancer and several networking components. The environment currently contains five EC2 instances.

Why this matters

Outdated documentation makes troubleshooting, onboarding, change planning, and incident response more difficult.

DemarkoCloud recommendation

Create an updated architecture diagram and maintain basic infrastructure documentation that reflects the production environment.

30 / 60 / 90-Day Roadmap

Timeframe	Objective	Recommended Actions
0-30 Days	Reduce Risk	Validate former privileged access and dependencies; review unrestricted administrative network exposure; plan and execute a controlled recovery-validation exercise.
31-60 Days	Improve Visibility	Establish appropriate CloudWatch monitoring and alerting; begin deeper document-management performance investigation; update the AWS architecture diagram.
61-90 Days	Optimize	Evaluate EC2 rightsizing using appropriate workload data; review AWS cost trends; evaluate whether selected infrastructure would benefit from Infrastructure as Code.

Why Infrastructure as Code appears later: Terraform is a capability DemarkoCloud can provide, but the assessment does not assume that every existing resource should immediately be converted to Infrastructure as Code.

Assessment Scope & Limitations

This demonstration assessment was structured as a read-only review. No production configuration changes were performed.

Not included: IAM account removal; security-group modification; EC2 resizing; application remediation; database tuning; production restoration; infrastructure migration; Terraform implementation; or ongoing managed services.

Any implementation activity resulting from these recommendations requires appropriate authorization and may require a separately defined scope of work.

Recommended Next Engagement

AWS Risk Reduction & Recovery Validation

Objective: Address the highest-priority findings identified during the Cloud Foundation & Architecture Review.

Potential scope: privileged-access remediation, administrative-access hardening, controlled recovery testing, baseline CloudWatch monitoring, and updated architecture documentation.

Separate workstreams: cost optimization and application-performance remediation remain separate until sufficient investigation supports specific changes.

This report is a fictional demonstration created to illustrate the structure, reasoning, and presentation of a DemarkoCloud AWS assessment. BlueRiver Accounting LLC is not represented as an actual DemarkoCloud client.