



AWS Well-Architected Tool

AWS Well-Architected Tool Render - AWS Well- Architected Framework Report

AWS Account ID: 0123456789123

AWS Well-Architected Tool Report

Copyright © 2020 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

All information, guidance and materials (collectively, "Information") provided to you in connection with the Program are for informational purposes only. You are solely responsible for making your own independent assessment of the Information and your use of AWS's products or services. Neither this document nor any other Information provided to you creates any warranties (express or implied), representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. Neither this document nor any other information provided to you are part of, nor do they modify, any agreements between you and AWS. All information in this document will be shared with only the Customer and the AWS Team.

Table of contents

Workload properties	4
Lens overview	5
Improvement plan	6
High risk	6
Medium risk	7
Lens details	9
Operational Excellence	9
Security	19
Reliability	31
Performance Efficiency	42
Cost Optimization	51

Workload properties

Workload name

Render

ARN

arn:aws:wellarchitected:us-west-2:0123456789123:workload/
dd2959b824ab7ffc191f2de7a830b9a5

Description

Encore render

Review owner

jeff@p1technologies.com

Industry type

Media & Entertainment

Industry

Content Production

Environment

Production

AWS Regions

US West (Oregon)

Non-AWS regions

-

Account IDs

0123456789123

Architectural design

-

Lens overview

Questions answered

46/46

Pillar	Questions answered
Operational Excellence	9/9
Security	11/11
Reliability	9/9
Performance Efficiency	8/8
Cost Optimization	9/9

Lens notes

-

Improvement plan

Improvement item summary

High risk: 14

Medium risk: 9

Pillar	High risk	Medium risk
Security	1	5
Reliability	2	2
Operational Excellence	4	0
Performance Efficiency	4	1
Cost Optimization	3	1

High risk

Security

- [SEC 11.How do you respond to an incident?](#)

Reliability

- [REL 7.How does your system withstand component failures?](#)
- [REL 1.How do you manage service limits?](#)

Operational Excellence

- OPS 1.How do you determine what your priorities are?
- OPS 2.How do you design your workload so that you can understand its state?
- OPS 4.How do you mitigate deployment risks?
- OPS 9.How do you evolve operations?

Performance Efficiency

- PERF 7.How do you monitor your resources to ensure they are performing as expected?
- PERF 2.How do you select your compute solution?
- PERF 5.How do you configure your networking solution?
- PERF 8.How do you use tradeoffs to improve performance?

Cost Optimization

- COST 1.How do you govern usage?
- COST 2.How do you monitor usage and cost?
- COST 9.How do you evaluate new services?

Medium risk

Security

- SEC 1.How do you manage credentials and authentication?
- SEC 4.How do you detect and investigate security events?
- SEC 2.How do you control human access?
- SEC 3.How do you control programmatic access?
- SEC 5.How do you defend against emerging security threats?

Reliability

- REL 4.How do you monitor your resources?
- REL 8.How do you test resilience?

Operational Excellence

No improvements identified

Performance Efficiency

- PERF 6.How do you evolve your workload to take advantage of new releases?

Cost Optimization

- COST 7.How do you plan for data transfer charges?






Lens details

Operational Excellence

Questions answered

9/9

Question status

-  High risk: 4
-  Medium risk: 0
-  No improvements identified: 5
-  Not Applicable: 0
-  Unanswered: 0

Pillar notes

-

1. How do you determine what your priorities are?

⊗ High risk

Selected choice(s)

- Evaluate external customer needs
- Evaluate compliance requirements
- Evaluate threat landscape
- Evaluate tradeoffs
- Manage benefits and risks

Not selected choice(s)

- Evaluate internal customer needs
- None of these

Notes

All components must meet MPAA compliance requirements which are non negotiable. All other priorities are primarily driven by delivery deadlines.

Improvement plan

- Understand business needs
- Understand compliance requirements
- Evaluate threat landscape
- Evaluate tradeoffs
- Manage benefits and risks

2. How do you design your workload so that you can understand its state?

⊗ High risk

Selected choice(s)

- Implement application telemetry
- Implement dependency telemetry
- Implement transaction traceability

Not selected choice(s)

- Implement and configure workload telemetry
- Implement user activity telemetry
- None of these

Notes

There's a hand-off between us and p1 teams related to control and insight to the render. The job management and queuing system will provide the most insight into operational health but logs sent to the elasticsearch system should be considered as well.

Improvement plan

- [Implement log and metric telemetry](#)
- [Implement transaction traceability](#)

3. How do you reduce defects, ease remediation, and improve flow into production?

✔ No improvements identified

Selected choice(s)

- Use version control
- Test and validate changes
- Use configuration management systems
- Share design standards
- Use multiple environments
- Make frequent, small, reversible changes
- Fully automate integration and deployment

Not selected choice(s)

- Use build and deployment management systems
- Perform patch management
- Implement practices to improve code quality
- None of these

Notes

consider config to put controls in place on resource deployment

Improvement plan

No risk detected for this question. No action needed.

4. How do you mitigate deployment risks?

⊗ High risk

Selected choice(s)

- Test and validate changes
- Test using limited deployments
- Deploy using parallel environments
- Deploy frequent, small, reversible changes
- Fully automate integration and deployment
- Automate testing and rollback

Not selected choice(s)

- Plan for unsuccessful changes
- Use deployment management systems
- None of these

Notes

Cloudformation output should be examined. Deployment process will be migrated from CF to Terraform where state and history will be captured in Terraform cloud.

Improvement plan

- [Plan for unsuccessful changes](#)
- [Use deployment management systems](#)
- [Test and validate changes](#)

5. How do you know that you are ready to support a workload?

✔ No improvements identified

Selected choice(s)

- Ensure personnel capability
- Ensure consistent review of operational readiness
- Use runbooks to perform procedures
- Use playbooks to identify issues
- Make informed decisions to deploy systems and changes

Not selected choice(s)

- None of these

Notes

-

Improvement plan

No risk detected for this question. No action needed.

6. How do you understand the health of your workload?

✔ No improvements identified

Selected choice(s)

- Identify key performance indicators
- Define workload metrics
- Collect and analyze workload metrics
- Establish workload metrics baselines
- Learn expected patterns of activity for workload
- Alert when workload outcomes are at risk
- Alert when workload anomalies are detected
- Validate the achievement of outcomes and the effectiveness of KPIs and metrics

Not selected choice(s)

- None of these

Notes

-

Improvement plan

No risk detected for this question. No action needed.

7. How do you understand the health of your operations?

✔ No improvements identified

Selected choice(s)

- Identify key performance indicators
- Define operations metrics
- Collect and analyze operations metrics
- Establish operations metrics baselines
- Learn the expected patterns of activity for operations
- Alert when operations outcomes are at risk
- Alert when operations anomalies are detected
- Validate the achievement of outcomes and the effectiveness of KPIs and metrics

Not selected choice(s)

- None of these

Notes

-

Improvement plan

No risk detected for this question. No action needed.

8. How do you manage workload and operations events?

✔ No improvements identified

Selected choice(s)

- Use processes for event, incident, and problem management
- Use a process for root cause analysis
- Have a process per alert
- Define escalation paths
- Automate responses to events

Not selected choice(s)

- Prioritize operational events based on business impact
- Enable push notifications
- Communicate status through dashboards
- None of these

Notes

-

Improvement plan

No risk detected for this question. No action needed.

9. How do you evolve operations?

⊗ High risk

Selected choice(s)

- Have a process for continuous improvement
- Define drivers for improvement
- Validate insights
- Document and share lessons learned
- Allocate time to make improvements

Not selected choice(s)

- Implement feedback loops
- Perform operations metrics reviews
- None of these

Notes

-

Improvement plan

- Define processes for continuous improvement
- Feedback loops
- Understand drivers for improvement
- Document and share lessons learned
- Allocate time to make improvements

Security

Questions answered

11/11

Question status

- ⊗ High risk: 1
- ⚠ Medium risk: 5
- ✔ No improvements identified: 3
- ⊖ Not Applicable: 2
- ⏸ Unanswered: 0

Pillar notes

-

1. How do you manage credentials and authentication?

 Medium risk

Selected choice(s)

- Define identity and access management requirements
- Secure AWS root user
- Enforce use of multi-factor authentication
- Enforce password requirements
- Rotate credentials regularly
- Audit credentials periodically

Not selected choice(s)

- Automate enforcement of access controls
- Integrate with centralized federation provider
- None of these

Notes

guard duty as an insurance policy

make logging into a root a noisy event

config to prevent root's ability to deploy resources

Improvement plan

- [Define credential and authentication management requirements](#)
- [Protect AWS accounts](#)
- [Secure credentials](#)
- [Use services and tools](#)

2. How do you control human access?

 Medium risk

Selected choice(s)

- Define human access requirements
- Grant least privileges
- Allocate unique credentials for each individual
- Manage credentials based on user lifecycles
- Automate credential management

Not selected choice(s)

- Grant access through roles or federation
- None of these

Notes

-

Improvement plan

- [Define human identity and access management requirements](#)
- [Configure user access](#)
- [IAM specific configuration](#)
- [Remove insecure configurations](#)

3. How do you control programmatic access?

 Medium risk

Selected choice(s)

- Define programmatic access requirements
- Grant least privileges
- Automate credential management

Not selected choice(s)

- Allocate unique credentials for each component
- Grant access through roles or federation
- Implement dynamic authentication
- None of these

Notes

-

Improvement plan

- [Define programmatic identity and access management requirements](#)
- [Configure programmatic access](#)
- [Remove insecure configurations](#)

4. How do you detect and investigate security events?

 Medium risk

Selected choice(s)

- Define requirements for logs
- Define requirements for metrics
- Define requirements for alerts
- Configure service and application logging
- Automate alerting on key indicators

Not selected choice(s)

- Analyze logs centrally
- Develop investigation processes
- None of these

Notes

review cloudcheckr alerts for changes
consider centralized log analysis, eg kibana

Improvement plan

- [Define security event detection and handling requirements](#)
- [Implement detective controls](#)
- [Implement investigation techniques](#)

5. How do you defend against emerging security threats?

 Medium risk

Selected choice(s)

- Keep up to date with organizational, legal, and compliance requirements
- Keep up to date with security best practices
- Keep up to date with security threats
- Evaluate new security services and features regularly
- Define and prioritize risks using a threat model

Not selected choice(s)

- Implement new security services and features
- None of these

Notes

identify ec2 instances that weren't started via CF

Improvement plan

- [Plan your defense](#)
- [Implement defense mechanisms](#)

6. How do you protect your networks?

✔ No improvements identified

Selected choice(s)

- Define network protection requirements
- Limit exposure
- Automate configuration management
- Automate network protection
- Implement inspection and protection
- Control traffic at all layers

Not selected choice(s)

- None of these

Notes

-

Improvement plan

No risk detected for this question. No action needed.

7. How do you protect your compute resources?

✔ No improvements identified

Selected choice(s)

- Define compute protection requirements
- Scan for and patch vulnerabilities
- Automate compute protection
- Reduce attack surface
- Implement managed services

Not selected choice(s)

- Automate configuration management
- None of these

Notes

-

Improvement plan

No risk detected for this question. No action needed.

8. How do you classify your data?

Not Applicable

Selected choice(s)

-

Not selected choice(s)

- Define data classification requirements
- Define data protection controls
- Implement data identification
- Automate identification and classification
- Identify the types of data
- None of these

Notes

consider as incident response plan

Improvement plan

Answer the question to view the improvement plan.

9. How do you protect your data at rest?

Not Applicable

Selected choice(s)

-

Not selected choice(s)

- Define data management and protection at rest requirements
- Implement secure key management
- Enforce encryption at rest
- Enforce access control
- Provide mechanisms to keep people away from data
- None of these

Notes

-

Improvement plan

Answer the question to view the improvement plan.

10. How do you protect your data in transit?

✔ No improvements identified

Selected choice(s)

- Define data protection in transit requirements
- Implement secure key and certificate management
- Enforce encryption in transit
- Automate detection of data leak
- Authenticate network communications

Not selected choice(s)

- None of these

Notes

-

Improvement plan

No risk detected for this question. No action needed.

11. How do you respond to an incident?

⊗ High risk

Selected choice(s)

- Identify tooling
- Automate containment capability
- Identify forensic capabilities

Not selected choice(s)

- Identify key personnel and external resources
- Develop incident response plans
- Pre-provision access
- Pre-deploy tools
- Run game days
- None of these

Notes

The deployment to burst render was done quickly and in an agile manner. While security standards were met, the environment sits outside of the Security teams purview.

Account resources should be migrated into a dedicated account within the existing AWS organization with cross account roles that enable access from the security account.

Improvement plan






- [Identify people who will respond to an incident](#)
- [Prepare for an incident](#)
- [Practice incident response and recovery](#)

Reliability

Questions answered

9/9

Question status

-  High risk: 2
-  Medium risk: 2
-  No improvements identified: 3
-  Not Applicable: 2
-  Unanswered: 0

Pillar notes

-

1. How do you manage service limits?

⊗ High risk

Selected choice(s)

- Aware of limits but not tracking them
- Monitor and manage limits
- Ensure a sufficient gap between the current service limit and the maximum usage to accommodate failover
- Manage service limits across all relevant accounts and regions

Not selected choice(s)

- Use automated monitoring and management of limits
- Accommodate fixed service limits through architecture
- None of these

Notes

There are a set of instance types that we will render using, including gpu instance types. We plan to raise those limits significantly by working with support. The ability to scale quickly is worth the tradeoff in not having a cap on potential abuse.

Improvement plan

- Identify service limits across all relevant accounts, regions, and Availability Zones
- Monitor and manage your limits
- Be aware of fixed service limits
- Ensure there is a sufficient gap between your service limit and your max usage to accommodate for fail over
- Set up automated monitoring

2. How do you manage your network topology?

✔ No improvements identified

Selected choice(s)

- Use highly available connectivity between private addresses in public clouds and on-premises environment
- Use highly available network connectivity for the users of the workload
- Enforce non-overlapping private IP address ranges in multiple private address spaces where they are connected
- Ensure IP subnet allocation accounts for expansion and availability

Not selected choice(s)

- None of these

Notes

-

Improvement plan

No risk detected for this question. No action needed.

3. How does your system adapt to changes in demand?

✔ No improvements identified

Selected choice(s)

- Procure resources automatically when scaling a workload up or down
- Procure resources upon detection of lack of service within a workload
- Load test the workload

Not selected choice(s)

- Procure resources manually upon detection that more resources may be needed soon for a workload
- None of these

Notes

load response

load test completed by Encore

Improvement plan

No risk detected for this question. No action needed.

4. How do you monitor your resources?

 Medium risk

Selected choice(s)

- Monitor the workload in all tiers
- Send notifications based on the monitoring
- Conduct reviews regularly

Not selected choice(s)

- Perform automated responses on events
- None of these

Notes

-

Improvement plan

- [Enable logging where available](#)
- [Consume all default metrics](#)
- [Create custom metrics for your own use](#)
- [Aggregate your logs](#)
- [Perform real-time processing and alarming](#)

5. How do you implement change?

✔ No improvements identified

Selected choice(s)

- Deploy changes in a planned manner
- Deploy changes with automation

Not selected choice(s)

- None of these

Notes

use config in a passive mode to document changes

Improvement plan

No risk detected for this question. No action needed.

6. How do you back up data?

Not Applicable

Selected choice(s)

-

Not selected choice(s)

- Identify all data that needs to be backed up and perform backups or reproduce the data from sources
- Perform data backup automatically or reproduce the data from sources automatically
- Perform periodic recovery of the data to verify backup integrity and processes
- Secure and encrypt backups or ensure the data is available from a secure source for reproduction
- None of these

Notes

-

Improvement plan

Answer the question to view the improvement plan.

7. How does your system withstand component failures?

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Monitor all layers of the workload to detect failures
- Implement loosely coupled dependencies
- Implement graceful degradation to transform applicable hard dependencies into soft dependencies
- Automating complete recovery because technology constraints exist in parts or all of the workload requiring a single location
- Deploy the workload to multiple locations
- Automate healing on all layers
- Send notifications upon availability impacting events

Notes

Failures are largely managed via the job management and queuing system. Although restarts and resubmits are appropriate responses to failure, it's important to identify failures quickly in the process. Frames produced over time is a possible metric to alert on it. Thresholds must be adjusted by job type.

Improvement plan

- [Use multiple Availability Zones and AWS Regions](#)
- [Make your applications stateless](#)
- [Decompose your services into smallest possible services](#)
- [Use distributed systems best practices](#)

7. How does your system withstand component failures?

- [Implement self healing](#)

8. How do you test resilience?

 Medium risk

Selected choice(s)

- Use playbooks for unanticipated failures
- Conduct root cause analysis (RCA) and share results

Not selected choice(s)

- Inject failures to test resiliency
- Conduct game days regularly
- None of these

Notes

-

Improvement plan

- [Prepare playbook and runbook formats](#)
- [Perform load testing](#)
- [Perform performance testing](#)
- [Perform failure injection testing](#)
- [Schedule game days to regularly exercise your runbooks and playbooks](#)
- [Establish a standard for your root cause analysis](#)

9. How do you plan for disaster recovery?

Not Applicable

Selected choice(s)

- Define recovery objectives for downtime and data loss
- Automate recovery

Not selected choice(s)

- Use defined recovery strategies to meet the recovery objectives
- Test disaster recovery implementation to validate the implementation
- Manage configuration drift on all changes
- None of these

Notes

s3 bucket with cloudformation templates outside of the acct

Improvement plan






Answer the question to view the improvement plan.

Performance Efficiency

Questions answered

8/8

Question status

-  High risk: 4
-  Medium risk: 1
-  No improvements identified: 2
-  Not Applicable: 1
-  Unanswered: 0

Pillar notes

-

1. How do you select the best performing architecture?

✔ No improvements identified

Selected choice(s)

- Understand the available services and resources
- Define a process for architectural choices
- Factor cost or budget into decisions
- Use policies or reference architectures
- Use guidance from AWS or an APN Partner
- Benchmark existing workloads
- Load test your workload

Not selected choice(s)

- None of these

Notes

-

Improvement plan

No risk detected for this question. No action needed.

2. How do you select your compute solution?

⊗ High risk

Selected choice(s)

- Evaluate the available compute options
- Collect compute-related metrics
- Determine the required configuration by right-sizing
- Use the available elasticity of resources

Not selected choice(s)

- Understand the available compute configuration options
- Re-evaluate compute needs based on metrics
- None of these

Notes

Existing instance sizing was based on testing of instance sizes using the same job submission and comparison of run times. GPU based instances were not included in this test. The scope of the test should be expanded to include both GPU and AMD based instances. Test results and conclusions should drive limit increase requests.

Improvement plan

- [Define compute performance requirements](#)
- [Consider compute options](#)
- [Learn about available configuration options](#)
- [Determine the required configuration by right-sizing](#)
- [Collect compute-related metrics](#)
- [Take advantage of elasticity](#)
- [Use a data-driven approach to optimize resources](#)

3. How do you select your storage solution?

✔ No improvements identified

Selected choice(s)

- Understand storage characteristics and requirements
- Evaluate available configuration options
- Make decisions based on access patterns and metrics

Not selected choice(s)

- None of these

Notes

-

Improvement plan

No risk detected for this question. No action needed.

4. How do you select your database solution?

Not Applicable

Selected choice(s)

-

Not selected choice(s)

- Understand data characteristics
- Evaluate the available options
- Collect and record database performance metrics
- Choose data storage based on access patterns
- Optimize data storage based on access patterns and metrics
- None of these

Notes

-

Improvement plan

Answer the question to view the improvement plan.

5. How do you configure your networking solution?

⊗ High risk

Selected choice(s)

- Understand available product options
- Leverage encryption offloading and load-balancing
- Choose location based on network requirements

Not selected choice(s)

- Understand how networking impacts performance
- Evaluate available networking features
- Use minimal network ACLs
- Choose network protocols to improve performance
- Optimize network configuration based on metrics
- None of these

Notes

May considering employing NACLs for unused services.

Improvement plan

- Define networking performance requirements
- Understand how your workload is impacted by the network
- Understand the available product options
- Select locations to reduce latency
- Use networking features
- Optimize traffic

6. How do you evolve your workload to take advantage of new releases?

 Medium risk

Selected choice(s)

- Keep up-to date on new resources and services

Not selected choice(s)

- Define a process to improve workload performance
- Evolve workload performance over time
- None of these

Notes

consider peer review

Improvement plan

- [Know the key performance constraints for your workload](#)
- [Evaluate updates and releases](#)
- [Evolve your workload over time](#)

7. How do you monitor your resources to ensure they are performing as expected?

 High risk

Selected choice(s)

- Record performance-related metrics
- Use monitoring to generate alarm-based notifications
- Review metrics at regular intervals
- Monitor and alarm proactively

Not selected choice(s)

- Analyze metrics when events or incidents occur
- Establish KPIs to measure workload performance
- None of these

Notes

-

Improvement plan

- [Record performance data](#)
- [Monitor performance during operations](#)

8. How do you use tradeoffs to improve performance?

⊗ High risk

Selected choice(s)

- Understand the areas where performance is most critical
- Use various performance-related strategies

Not selected choice(s)

- Learn about design patterns and services
- Identify how tradeoffs impact customers and efficiency
- Measure the impact of performance improvements
- None of these

Notes

Analysis of job queues and run times should be added to process.
Need to develop clear understanding of renders completed relative to time/cost.

Improvement plan






- Identify hotspots
- Identify tradeoffs
- Use a combination of strategies
- Use a data-driven approach to evolve your architecture

Cost Optimization

Questions answered

9/9

Question status

-  High risk: 3
-  Medium risk: 1
-  No improvements identified: 5
-  Not Applicable: 0
-  Unanswered: 0

Pillar notes

-

1. How do you govern usage?

⊗ High risk

Selected choice(s)

- Implement an account structure
- Implement groups and roles
- Implement cost controls

Not selected choice(s)

- Develop policies based on your organization requirements
- Track project lifecycle
- None of these

Notes

Budgets and Cloudcheckr alerts should be implemented as notifications of spending increase as a percentage of daily spend. New services deployment notifications should also be configured (via Cloudcheckr).

Improvement plan

- Define financial and optimization goals for accounts and workloads
- Implement an account structure
- Create IAM policies to control resource creation
- Review the cost effectiveness of the workload
- Use service limits to control cost

2. How do you monitor usage and cost?

⊗ High risk

Selected choice(s)

- Configure AWS Cost and Usage Report
- Identify cost attribution categories
- Define and implement tagging
- Configure billing and cost management tools
- Monitor cost proactively

Not selected choice(s)

- Establish organization metrics
- Report and notify on cost optimization
- Allocate costs based on workload metrics
- None of these

Notes

Analysis of select Cloudcheckr reports (currently too much noise) should be driven by notifications sent based on a percentage of increased spend.

Improvement plan

- [Define a tagging schema for your organization](#)
- [Configure AWS Budgets](#)
- [Configure Cost Explorer](#)
- [Enable AWS Cost and Usage Report](#)

3. How do you decommission resources?

✔ No improvements identified

Selected choice(s)

- Track resources over their life time
- Implement a decommissioning process
- Decommission resources automatically

Not selected choice(s)

- Decommission resources in an unplanned manner
- None of these

Notes

-

Improvement plan

No risk detected for this question. No action needed.

4. How do you evaluate cost when you select services?

✔ No improvements identified

Selected choice(s)

- Identify organization requirements for cost
- Analyze all components of this workload
- Perform a thorough analysis of each component
- Select components of this workload to optimize cost inline with organization priorities
- Perform cost analysis for different usage over time

Not selected choice(s)

- None of these

Notes

-

Improvement plan

No risk detected for this question. No action needed.

5. How do you meet cost targets when you select resource type and size?

✔ No improvements identified

Selected choice(s)

- Perform cost modeling
- Select resource type and size based on estimates
- Select resource type and size based on metrics

Not selected choice(s)

- None of these

Notes

-

Improvement plan

No risk detected for this question. No action needed.

6. How do you use pricing models to reduce cost?

✔ No improvements identified

Selected choice(s)

- Perform pricing model analysis
- Implement regions based on cost
- Implement pricing models for all components of this workload

Not selected choice(s)

- Implement different pricing models, with low coverage
- None of these

Notes

-

Improvement plan

No risk detected for this question. No action needed.

7. How do you plan for data transfer charges?

 Medium risk

Selected choice(s)

- Perform data transfer modeling

Not selected choice(s)

- Select components to optimize data transfer cost
- Implement services to reduce data transfer costs
- None of these

Notes

-

Improvement plan

- [Model data transfer costs throughout a workload](#)
- [Review data transfer costs](#)
- [Configure Amazon CloudFront for larger traffic volumes](#)
- [Implement caching layers](#)
- [Use AWS Direct Connect instead of VPN](#)

8. How do you match supply of resources with demand?

✔ No improvements identified

Selected choice(s)

- Perform an analysis on the workload demand
- Provision resources dynamically

Not selected choice(s)

- Provision resources reactively or unplanned
- None of these

Notes

-

Improvement plan

No risk detected for this question. No action needed.

9. How do you evaluate new services?

⊗ High risk

Selected choice(s)

- Establish a cost optimization function
- Review and analyze this workload regularly
- Keep up to date with new service releases

Not selected choice(s)

- Develop a workload review process
- Review and implement services in an unplanned way
- None of these

Notes

Cloudcheckr new service deployment notifications are critical.

Improvement plan

- [Establish a cost optimization function](#)
- [Subscribe to the AWS What's New announcements](#)
- [Attend AWS user or Meetup groups](#)
- [Review current workload architectures](#)