



AWS Well-Architected Tool

AWS Well-Architected Tool

jpwelby0011223344 -

AWS Well-Architected Framework Report

AWS Account ID: 447746619643

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	9
Lens details	11
Operational Excellence	11
Security	30
Reliability	43
Performance Efficiency	59
Cost Optimization	70

Workload properties

Workload name

jpwelby0011223344

ARN

arn:aws:wellarchitected:us-east-1:447746619643:workload/
b87ba0692efd9e3101e894dc4f919880

Description

test workload to learn how to use the AWS Well-Architected Tool

Review owner

marzetti65@gmail.com

Industry type

Defense

Industry

Defense

Environment

Pre-production

AWS Regions

US East (N. Virginia)

Non-AWS regions

-

Account IDs

-

Architectural design

Lens overview

Questions answered

52/52

Version

AWS Well-Architected Framework, 2nd Jul 2020

Pillar	Questions answered
Operational Excellence	11/11
Security	10/10
Reliability	13/13
Performance Efficiency	8/8
Cost Optimization	10/10

Lens notes

-

Improvement plan

Improvement item summary

High risk: 52

Medium risk: 0

Pillar	High risk	Medium risk
Security	10	0
Reliability	13	0
Operational Excellence	11	0
Performance Efficiency	8	0
Cost Optimization	10	0

High risk

Security

- [SEC 1.How do you securely operate your workload?](#)
- [SEC 2.How do you manage identities for people and machines?](#)
- [SEC 3.How do you manage permissions for people and machines?](#)
- [SEC 4.How do you detect and investigate security events?](#)
- [SEC 5.How do you protect your network resources?](#)
- [SEC 6.How do you protect your compute resources?](#)
- [SEC 7.How do you classify your data?](#)
- [SEC 8.How do you protect your data at rest?](#)
- [SEC 9.How do you protect your data in transit?](#)
- [SEC 10.How do you anticipate, respond to, and recover from incidents?](#)

Reliability

- REL 9.How do you back up data?
- REL 6.How do you monitor workload resources?
- REL 12.How do you test reliability?
- REL 8.How do you implement change?
- REL 10.How do you use fault isolation to protect your workload?
- REL 11.How do you design your workload to withstand component failures?
- REL 2.How do you plan your network topology?
- REL 13.How do you plan for disaster recovery (DR)?
- REL 7.How do you design your workload to adapt to changes in demand?
- REL 5.How do you design interactions in a distributed system to mitigate or withstand failures?
- REL 4.How do you design interactions in a distributed system to prevent failures?
- REL 3.How do you design your workload service architecture?
- REL 1.How do you manage service quotas and constraints?

Operational Excellence

- OPS 1. How do you determine what your priorities are?
- OPS 2. How do you structure your organization to support your business outcomes?
- OPS 3. How does your organizational culture support your business outcomes?
- OPS 4. How do you design your workload so that you can understand its state?
- OPS 5. How do you reduce defects, ease remediation, and improve flow into production?
- OPS 6. How do you mitigate deployment risks?
- OPS 7. How do you know that you are ready to support a workload?
- OPS 8. How do you understand the health of your workload?
- OPS 9. How do you understand the health of your operations?
- OPS 10. How do you manage workload and operations events?
- OPS 11. How do you evolve operations?

Performance Efficiency

- PERF 1.How do you select the best performing architecture?
- PERF 7.How do you monitor your resources to ensure they are performing?
- PERF 2.How do you select your compute solution?
- PERF 3.How do you select your storage solution?
- PERF 4.How do you select your database solution?
- PERF 5.How do you configure your networking solution?
- PERF 6.How do you evolve your workload to take advantage of new releases?
- PERF 8.How do you use tradeoffs to improve performance?

Cost Optimization

- COST 1.How do you implement cloud financial management?
- COST 2.How do you govern usage?
- COST 3.How do you monitor usage and cost?
- COST 10.How do you evaluate new services?
- COST 5.How do you evaluate cost when you select services?
- COST 6.How do you meet cost targets when you select resource type, size and number?
- COST 7.How do you use pricing models to reduce cost?
- COST 9.How do you manage demand, and supply resources?
- COST 8.How do you plan for data transfer charges?
- COST 4.How do you decommission resources?

Medium risk

Security
No improvements identified

Reliability
No improvements identified

Operational Excellence
No improvements identified

Performance Efficiency
No improvements identified

Cost Optimization
No improvements identified






Lens details

Operational Excellence

Questions answered

11/11

Question status

-  High risk: 11
-  Medium risk: 0
-  No improvements identified: 0
-  Not Applicable: 0
-  Unanswered: 0

Pillar notes

-

1. How do you determine what your priorities are?

⊗ High risk

Selected choice(s)

- Evaluate internal customer needs
- Evaluate governance requirements
- Evaluate compliance requirements
- Evaluate threat landscape
- Manage benefits and risks

Not selected choice(s)

- Evaluate external customer needs
- Evaluate tradeoffs
- None of these

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- Evaluate external customer needs
- Evaluate tradeoffs

2. How do you structure your organization to support your business outcomes?

⊗ High risk

Selected choice(s)

- Team members know what they are responsible for

Not selected choice(s)

- Resources have identified owners
- Processes and procedures have identified owners
- Operations activities have identified owners responsible for their performance
- Mechanisms exist to identify responsibility and ownership
- Mechanisms exist to request additions, changes, and exceptions
- Responsibilities between teams are predefined or negotiated
- None of these

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- Resources have identified owners
- Processes and procedures have identified owners
- Operations activities have identified owners responsible for their performance
- Mechanisms exist to identify responsibility and ownership

2. How do you structure your organization to support your business outcomes?

- Mechanisms exist to request additions, changes, and exceptions
- Responsibilities between teams are predefined or negotiated

3. How does your organizational culture support your business outcomes?

⊗ High risk

Selected choice(s)

- Resource teams appropriately

Not selected choice(s)

- Executive Sponsorship
- Team members are empowered to take action when outcomes are at risk
- Escalation is encouraged
- Communications are timely, clear, and actionable
- Experimentation is encouraged
- Team members are enabled and encouraged to maintain and grow their skill sets
- Diverse opinions are encouraged and sought within and across teams
- None of these

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- [Executive Sponsorship](#)
- [Team members are empowered to take action when outcomes are at risk](#)
- [Escalation is encouraged](#)
- [Communications are timely, clear, and actionable](#)

3. How does your organizational culture support your business outcomes?

- Experimentation is encouraged
- Team members are enabled and encouraged to maintain and grow their skill sets
- Diverse opinions are encouraged and sought within and across teams

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

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Implement application telemetry
- Implement and configure workload telemetry
- Implement user activity telemetry
- Implement dependency telemetry
- Implement transaction traceability

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- [Implement application telemetry](#)
- [Implement and configure workload telemetry](#)
- [Implement user activity telemetry](#)
- [Implement dependency telemetry](#)
- [Implement transaction traceability](#)

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

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Use version control
- Test and validate changes
- Use configuration management systems
- Use build and deployment management systems
- Perform patch management
- Share design standards
- Implement practices to improve code quality
- Use multiple environments
- Make frequent, small, reversible changes
- Fully automate integration and deployment

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- Use version control
- Test and validate changes
- Use configuration management systems

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

- Use build and deployment management systems
- Perform patch management
- Share design standards
- Implement practices to improve code quality
- Use multiple environments
- Make frequent, small, reversible changes
- Fully automate integration and deployment

6. How do you mitigate deployment risks?

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Plan for unsuccessful changes
- Test and validate changes
- Use deployment management systems
- Test using limited deployments
- Deploy using parallel environments
- Deploy frequent, small, reversible changes
- Fully automate integration and deployment
- Automate testing and rollback

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- Plan for unsuccessful changes
- Test and validate changes
- Use deployment management systems
- Test using limited deployments
- Deploy using parallel environments
- Deploy frequent, small, reversible changes

6. How do you mitigate deployment risks?

- Fully automate integration and deployment
- Automate testing and rollback

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

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

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

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

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

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

⊗ High risk

Selected choice(s)

- None of these

Not 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

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- Identify key performance indicators
- Define workload metrics
- Collect and analyze workload metrics

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

- 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

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

⊗ High risk

Selected choice(s)

- None of these

Not 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

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- Identify key performance indicators
- Define operations metrics
- Collect and analyze operations metrics

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

- 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

10. How do you manage workload and operations events?

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Use processes for event, incident, and problem management
- Have a process per alert
- Prioritize operational events based on business impact
- Define escalation paths
- Enable push notifications
- Communicate status through dashboards
- Automate responses to events

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- Use processes for event, incident, and problem management
- Have a process per alert
- Prioritize operational events based on business impact
- Define escalation paths
- Enable push notifications
- Communicate status through dashboards
- Automate responses to events

11. How do you evolve operations?

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Have a process for continuous improvement
- Perform post-incident analysis
- Implement feedback loops
- Perform Knowledge Management
- Define drivers for improvement
- Validate insights
- Perform operations metrics reviews
- Document and share lessons learned
- Allocate time to make improvements

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- Have a process for continuous improvement
- Perform post-incident analysis
- Implement feedback loops
- Perform Knowledge Management
- Define drivers for improvement

11. How do you evolve operations?






- Validate insights
- Perform operations metrics reviews
- Document and share lessons learned
- Allocate time to make improvements

Security

Questions answered

10/10

Question status

-  High risk: 10
-  Medium risk: 0
-  No improvements identified: 0
-  Not Applicable: 0
-  Unanswered: 0

Pillar notes

-

1. How do you securely operate your workload?

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Separate workloads using accounts
- Secure AWS account
- Identify and validate control objectives
- Keep up to date with security threats
- Keep up to date with security recommendations
- Automate testing and validation of security controls in pipelines
- Identify and prioritize risks using a threat model
- Evaluate and implement new security services and features regularly

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- Separate workloads using accounts
- Secure AWS account
- Identify and validate control objectives
- Keep up to date with security threats
- Keep up to date with security recommendations
- Automate testing and validation of security controls in pipelines

1. How do you securely operate your workload?

- Identify and prioritize risks using a threat model
- Evaluate and implement new security services and features regularly

2. How do you manage identities for people and machines?

⊗ High risk

Selected choice(s)

- Leverage user groups and attributes

Not selected choice(s)

- Use strong sign-in mechanisms
- Use temporary credentials
- Store and use secrets securely
- Rely on a centralized identity provider
- Audit and rotate credentials periodically
- None of these

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- Use strong sign-in mechanisms
- Use temporary credentials
- Store and use secrets securely
- Rely on a centralized identity provider
- Audit and rotate credentials periodically

3. How do you manage permissions for people and machines?

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Define access requirements
- Grant least privilege access
- Establish emergency access process
- Reduce permissions continuously
- Define permission guardrails for your organization
- Manage access based on life cycle
- Analyze public and cross account access
- Share resources securely

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- Define access requirements
- Grant least privilege access
- Establish emergency access process
- Reduce permissions continuously
- Define permission guardrails for your organization
- Manage access based on life cycle

3. How do you manage permissions for people and machines?

- Analyze public and cross account access
- Share resources securely

4. How do you detect and investigate security events?

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Configure service and application logging
- Analyze logs, findings, and metrics centrally
- Automate response to events
- Implement actionable security events

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- [Configure service and application logging](#)
- [Analyze logs, findings, and metrics centrally](#)
- [Automate response to events](#)
- [Implement actionable security events](#)

5. How do you protect your network resources?

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Create network layers
- Control traffic at all layers
- Automate network protection
- Implement inspection and protection

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- Create network layers
- Control traffic at all layers
- Automate network protection
- Implement inspection and protection

6. How do you protect your compute resources?

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Perform vulnerability management
- Reduce attack surface
- Implement managed services
- Automate compute protection
- Enable people to perform actions at a distance
- Validate software integrity

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- Perform vulnerability management
- Reduce attack surface
- Implement managed services
- Automate compute protection
- Enable people to perform actions at a distance
- Validate software integrity

7. How do you classify your data?

High risk

Selected choice(s)

- Define data protection controls

Not selected choice(s)

- Identify the data within your workload
- Automate identification and classification
- Define data lifecycle management
- None of these

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- Identify the data within your workload
- Automate identification and classification
- Define data lifecycle management

8. How do you protect your data at rest?

⊗ High risk

Selected choice(s)

- Enforce encryption at rest

Not selected choice(s)

- Implement secure key management
- Automate data at rest protection
- Enforce access control
- Use mechanisms to keep people away from data
- None of these

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- [Implement secure key management](#)
- [Automate data at rest protection](#)
- [Enforce access control](#)
- [Use mechanisms to keep people away from data](#)

9. How do you protect your data in transit?

⊗ High risk

Selected choice(s)

- Enforce encryption in transit

Not selected choice(s)

- Implement secure key and certificate management
- Automate detection of unintended data access
- Authenticate network communications
- None of these

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- [Implement secure key and certificate management](#)
- [Automate detection of unintended data access](#)
- [Authenticate network communications](#)

10. How do you anticipate, respond to, and recover from incidents?

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Identify key personnel and external resources
- Develop incident management plans
- Prepare forensic capabilities
- Automate containment capability
- Pre-provision access
- Pre-deploy tools
- Run game days

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan






- Identify key personnel and external resources
- Develop incident management plans
- Prepare forensic capabilities
- Automate containment capability
- Pre-provision access
- Pre-deploy tools
- Run game days

Reliability

Questions answered

13/13

Question status

-  High risk: 13
-  Medium risk: 0
-  No improvements identified: 0
-  Not Applicable: 0
-  Unanswered: 0

Pillar notes

-

1. How do you manage service quotas and constraints?

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Aware of service quotas and constraints
- Manage service quotas across accounts and regions
- Accommodate fixed service quotas and constraints through architecture
- Monitor and manage quotas
- Automate quota management
- Ensure that a sufficient gap exists between the current quotas and the maximum usage to accommodate failover

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- [Aware of service quotas and constraints](#)
- [Manage service quotas across accounts and regions](#)
- [Accommodate fixed service quotas and constraints through architecture](#)
- [Monitor and manage quotas](#)
- [Automate quota management](#)
- [Ensure that a sufficient gap exists between the current quotas and the maximum usage to accommodate failover](#)

2. How do you plan your network topology?

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Use highly available network connectivity for your workload public endpoints
- Provision redundant connectivity between private networks in the cloud and on-premises environments
- Ensure IP subnet allocation accounts for expansion and availability
- Prefer hub-and-spoke topologies over many-to-many mesh
- Enforce non-overlapping private IP address ranges in all private address spaces where they are connected

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- Use highly available network connectivity for your workload public endpoints
- Provision redundant connectivity between private networks in the cloud and on-premises environments
- Ensure IP subnet allocation accounts for expansion and availability
- Prefer hub-and-spoke topologies over many-to-many mesh

2. How do you plan your network topology?

- Enforce non-overlapping private IP address ranges in all private address spaces where they are connected

3. How do you design your workload service architecture?

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Choose how to segment your workload
- Build services focused on specific business domains and functionality
- Provide service contracts per API

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- Choose how to segment your workload
- Build services focused on specific business domains and functionality
- Provide service contracts per API

4. How do you design interactions in a distributed system to prevent failures?

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Identify which kind of distributed system is required
- Implement loosely coupled dependencies
- Make all responses idempotent
- Do constant work

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- Identify which kind of distributed system is required
- Implement loosely coupled dependencies
- Make all responses idempotent
- Do constant work

5. How do you design interactions in a distributed system to mitigate or withstand failures?

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Implement graceful degradation to transform applicable hard dependencies into soft dependencies
- Throttle requests
- Control and limit retry calls
- Fail fast and limit queues
- Set client timeouts
- Make services stateless where possible
- Implement emergency levers

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- Implement graceful degradation to transform applicable hard dependencies into soft dependencies
- Throttle requests
- Control and limit retry calls
- Fail fast and limit queues

5. How do you design interactions in a distributed system to mitigate or withstand failures?

- Set client timeouts
- Make services stateless where possible
- Implement emergency levers

6. How do you monitor workload resources?

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Monitor all components for the workload (Generation)
- Define and calculate metrics (Aggregation)
- Send notifications (Real-time processing and alarming)
- Automate responses (Real-time processing and alarming)
- Storage and Analytics
- Conduct reviews regularly
- Monitor end-to-end tracing of requests through your system

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- Monitor all components for the workload (Generation)
- Define and calculate metrics (Aggregation)
- Send notifications (Real-time processing and alarming)
- Automate responses (Real-time processing and alarming)
- Storage and Analytics
- Conduct reviews regularly
- Monitor end-to-end tracing of requests through your system

7. How do you design your workload to adapt to changes in demand?

High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Use automation when obtaining or scaling resources
- Obtain resources upon detection of impairment to a workload
- Obtain resources upon detection that more resources are needed for a workload
- Load test your workload

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- Use automation when obtaining or scaling resources
- Obtain resources upon detection of impairment to a workload
- Obtain resources upon detection that more resources are needed for a workload
- Load test your workload

8. How do you implement change?

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Use runbooks for standard activities such as deployment
- Integrate functional testing as part of your deployment
- Integrate resiliency testing as part of your deployment
- Deploy using immutable infrastructure
- Deploy changes with automation

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- Use runbooks for standard activities such as deployment
- Integrate functional testing as part of your deployment
- Integrate resiliency testing as part of your deployment
- Deploy using immutable infrastructure
- Deploy changes with automation

9. How do you back up data?

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Identify and back up all data that needs to be backed up, or reproduce the data from sources
- Secure and encrypt backups
- Perform data backup automatically
- Perform periodic recovery of the data to verify backup integrity and processes

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- Identify and back up all data that needs to be backed up, or reproduce the data from sources
- Secure and encrypt backups
- Perform data backup automatically
- Perform periodic recovery of the data to verify backup integrity and processes

10. How do you use fault isolation to protect your workload?

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Deploy the workload to multiple locations
- Automate recovery for components constrained to a single location
- Use bulkhead architectures

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- [Deploy the workload to multiple locations](#)
- [Automate recovery for components constrained to a single location](#)
- [Use bulkhead architectures](#)

11. How do you design your workload to withstand component failures?

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Monitor all components of the workload to detect failures
- Fail over to healthy resources
- Automate healing on all layers
- Use static stability to prevent bimodal behavior
- Send notifications when events impact availability

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- Monitor all components of the workload to detect failures
- Fail over to healthy resources
- Automate healing on all layers
- Use static stability to prevent bimodal behavior
- Send notifications when events impact availability

12. How do you test reliability?

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Use playbooks to investigate failures
- Perform post-incident analysis
- Test functional requirements
- Test scaling and performance requirements
- Test resiliency using chaos engineering
- Conduct game days regularly

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- Use playbooks to investigate failures
- Perform post-incident analysis
- Test functional requirements
- Test scaling and performance requirements
- Test resiliency using chaos engineering
- Conduct game days regularly

13. How do you plan for disaster recovery (DR)?

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Define recovery objectives for downtime and data loss
- Use defined recovery strategies to meet the recovery objectives
- Test disaster recovery implementation to validate the implementation
- Manage configuration drift at the DR site or region
- Automate recovery

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan






- Define recovery objectives for downtime and data loss
- Use defined recovery strategies to meet the recovery objectives
- Test disaster recovery implementation to validate the implementation
- Manage configuration drift at the DR site or region
- Automate recovery

Performance Efficiency

Questions answered

8/8

Question status

-  High risk: 8
-  Medium risk: 0
-  No improvements identified: 0
-  Not Applicable: 0
-  Unanswered: 0

Pillar notes

-

1. How do you select the best performing architecture?

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Understand the available services and resources
- Define a process for architectural choices
- Factor cost requirements into decisions
- Use policies or reference architectures
- Use guidance from your cloud provider or an appropriate partner
- Benchmark existing workloads
- Load test your workload

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- Understand the available services and resources
- Define a process for architectural choices
- Factor cost requirements into decisions
- Use policies or reference architectures
- Use guidance from your cloud provider or an appropriate partner
- Benchmark existing workloads
- Load test your workload

2. How do you select your compute solution?

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Evaluate the available compute options
- Understand the available compute configuration options
- Collect compute-related metrics
- Determine the required configuration by right-sizing
- Use the available elasticity of resources
- Re-evaluate compute needs based on metrics

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- Evaluate the available compute options
- Understand the available compute configuration options
- Collect compute-related metrics
- Determine the required configuration by right-sizing
- Use the available elasticity of resources
- Re-evaluate compute needs based on metrics

3. How do you select your storage solution?

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

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

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

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

4. How do you select your database solution?

⊗ High risk

Selected choice(s)

- None of these

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

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- 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

5. How do you configure your networking solution?

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Understand how networking impacts performance
- Evaluate available networking features
- Choose appropriately sized dedicated connectivity or VPN for hybrid workloads
- Leverage load-balancing and encryption offloading
- Choose network protocols to improve performance
- Choose your workload's location based on network requirements
- Optimize network configuration based on metrics

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- Understand how networking impacts performance
- Evaluate available networking features
- Choose appropriately sized dedicated connectivity or VPN for hybrid workloads
- Leverage load-balancing and encryption offloading
- Choose network protocols to improve performance

5. How do you configure your networking solution?

- Choose your workload's location based on network requirements
- Optimize network configuration based on metrics

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

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Stay up-to-date on new resources and services
- Define a process to improve workload performance
- Evolve workload performance over time

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- Stay up-to-date on new resources and services
- Define a process to improve workload performance
- Evolve workload performance over time

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

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Record performance-related metrics
- Analyze metrics when events or incidents occur
- Establish Key Performance Indicators (KPIs) to measure workload performance
- Use monitoring to generate alarm-based notifications
- Review metrics at regular intervals
- Monitor and alarm proactively

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- Record performance-related metrics
- Analyze metrics when events or incidents occur
- Establish Key Performance Indicators (KPIs) to measure workload performance
- Use monitoring to generate alarm-based notifications
- Review metrics at regular intervals

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

- [Monitor and alarm proactively](#)

8. How do you use tradeoffs to improve performance?

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Understand the areas where performance is most critical
- Learn about design patterns and services
- Identify how tradeoffs impact customers and efficiency
- Measure the impact of performance improvements
- Use various performance-related strategies

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan






- Understand the areas where performance is most critical
- Learn about design patterns and services
- Identify how tradeoffs impact customers and efficiency
- Measure the impact of performance improvements
- Use various performance-related strategies

Cost Optimization

Questions answered

10/10

Question status

-  High risk: 10
-  Medium risk: 0
-  No improvements identified: 0
-  Not Applicable: 0
-  Unanswered: 0

Pillar notes

-

1. How do you implement cloud financial management?

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Establish a cost optimization function
- Establish a partnership between finance and technology
- Establish cloud budgets and forecasts
- Implement cost awareness in your organizational processes
- Report and notify on cost optimization
- Monitor cost proactively
- Keep up to date with new service releases

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- Establish a cost optimization function
- Establish a partnership between finance and technology
- Establish cloud budgets and forecasts
- Implement cost awareness in your organizational processes
- Report and notify on cost optimization
- Monitor cost proactively
- Keep up to date with new service releases

2. How do you govern usage?

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Develop policies based on your organization requirements
- Implement goals and targets
- Implement an account structure
- Implement groups and roles
- Implement cost controls
- Track project lifecycle

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- [Develop policies based on your organization requirements](#)
- [Implement goals and targets](#)
- [Implement an account structure](#)
- [Implement groups and roles](#)
- [Implement cost controls](#)
- [Track project lifecycle](#)

3. How do you monitor usage and cost?

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Configure detailed information sources
- Identify cost attribution categories
- Establish organization metrics
- Configure billing and cost management tools
- Add organization information to cost and usage
- Allocate costs based on workload metrics

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- [Configure detailed information sources](#)
- [Identify cost attribution categories](#)
- [Establish organization metrics](#)
- [Configure billing and cost management tools](#)
- [Add organization information to cost and usage](#)
- [Allocate costs based on workload metrics](#)

4. How do you decommission resources?

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

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

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

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

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

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

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

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

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

6. How do you meet cost targets when you select resource type, size and number?

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Perform cost modeling
- Select resource type, size, and number based on data
- Select resource type, size, and number automatically based on metrics

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- Perform cost modeling
- Select resource type, size, and number based on data
- Select resource type, size, and number automatically based on metrics

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

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Perform pricing model analysis
- Implement regions based on cost
- Select third party agreements with cost efficient terms
- Implement pricing models for all components of this workload
- Perform pricing model analysis at the master account level

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- Perform pricing model analysis
- Implement regions based on cost
- Select third party agreements with cost efficient terms
- Implement pricing models for all components of this workload
- Perform pricing model analysis at the master account level

8. How do you plan for data transfer charges?

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Perform data transfer modeling
- Select components to optimize data transfer cost
- Implement services to reduce data transfer costs

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- Perform data transfer modeling
- Select components to optimize data transfer cost
- Implement services to reduce data transfer costs

9. How do you manage demand, and supply resources?

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Perform an analysis on the workload demand
- Implement a buffer or throttle to manage demand
- Supply resources dynamically

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- Perform an analysis on the workload demand
- Implement a buffer or throttle to manage demand
- Supply resources dynamically

10. How do you evaluate new services?

⊗ High risk

Selected choice(s)

- None of these

Not selected choice(s)

- Develop a workload review process
- Review and analyze this workload regularly

Best Practices marked as Not Applicable

-

Notes

-

Improvement plan

- [Develop a workload review process](#)
- [Review and analyze this workload regularly](#)

