AWS Well-Architected Tool CitizenIntelligenceAgencyProduction Review Report

AWS Account ID: 172017021075

AWS Well-Architected Tool: Workload Review Report

Table of contents

Workload properties

Workload name
CitizenIntelligenceAgencyProduction

ARN
arn:aws:wellarchitected:eu-west-1:172017021075:workload/b59aa7eace7ab1bc39d02d57ec8a9ed1

Description
Citizen Intelligence Agency::Tracking politicians like bugs.
Target subset of the visitors at
https://www.alexa.com/siteinfo/riksdagen.se
https://www.alexa.com/siteinfo/esv.se
https://www.alexa.com/siteinfo/altinget.se

Industry group
InfoTech

Sub-industry
Software

Regions
EU (Ireland)

Type
Pre-production

Account IDs
172017021075, 201366349527

Review overview

Status

Answered

Pillar status

Operational Excellence: Answered

Security: Answered

Reliability: Answered

Performance Efficiency: Answered

Cost Optimization: Answered

Improvement item summary

High risk: 30

Medium risk: 9

Pillar	High risk	Medium risk
Operational Excellence	5	1
Security	8	1
Reliability	7	2
Performance Efficiency	2	5
Cost Optimization	8	0

Review notes

-

Review details

Operational Excellence

Pillar status

Answered

Question status

Answered: 9

Not Applicable: 0

Unanswered: 0

Pillar notes

-

1. How do you determine what your priorities are?

Answered

Selected choices

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

Not selected choices

- None of these

Notes

Demo setup, public instance that allow users access to data without registration.

Database wiped occasionally.

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

Answered

Selected choices

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

Not selected choices

- Implement dependency telemetry
- None of these

Notes

Application pushes metrics(Javamelody) , system metrics & logs(syslog,auth,kern,lynis, user-data,cia-app) to cloudwatch
Application track usersessions and actions in application database.
Application uses JTA transactions for all operations.

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

Answered

Selected choices

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

Not selected choices

- Share design standards
- None of these

Notes

https://github.com/Hack23/cia
https://www.hack23.com/jenkins/view/Pipelines/job/CloudPipeline/
https://www.hack23.com/sonar/dashboard?id=com.hack23.cia%3Acia-all
SSM patch compliant OS,
Bots: Snyk, Dependabot,blackduck,depshield for app.

4. How do you mitigate deployment risks?

Answered

Selected choices

- Test and validate changes

Not selected choices

- Plan for unsuccessful 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
- None of these

Notes

Required before going live.

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

Answered

Selected choices

- None of these

Not selected choices

- 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

Notes

-

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

Answered

Selected choices

- None of these

Not selected choices

- 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

Notes

-

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

Answered

Selected choices

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

Not selected choices

- 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
- None of these

Notes

-

8. How do you manage workload and operations events?

Answered

Selected choices

- None of these

Not selected choices

- Use processes for event, incident, and problem management
- Use a process for root cause analysis
- 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

Notes

-

9. How do you evolve operations?

Answered

Selected choices

- Have a process for continuous improvement

Not selected choices

- Implement feedback loops
- Define drivers for improvement
- Validate insights
- Perform operations metrics reviews
- Document and share lessons learned
- Allocate time to make improvements
- None of these

Notes

-

Security

Pillar status

Answered

Question status

Answered: 11

Not Applicable: 0

Unanswered: 0

Pillar notes

-

1. How do you manage credentials and authentication?

Answered

Selected choices

- Secure AWS root user
- Enforce use of multi-factor authentication
- Automate enforcement of access controls
- Enforce password requirements
- Rotate credentials regularly
- Audit credentials periodically

Not selected choices

- Define identity and access management requirements
- Integrate with centralized federation provider
- None of these

Notes

-

2. How do you control human access?

Answered

Selected choices

- Grant least privileges
- Allocate unique credentials for each individual

Not selected choices

- Define human access requirements
- Manage credentials based on user lifecycles
- Automate credential management
- Grant access through roles or federation
- None of these

Notes

-

3. How do you control programmatic access?

Answered

Selected choices

- Grant least privileges
- Grant access through roles or federation

Not selected choices

- Define programmatic access requirements
- Automate credential management
- Allocate unique credentials for each component
- Implement dynamic authentication
- None of these

Notes

-

4. How do you detect and investigate security events?

Answered

Selected choices

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

Not selected choices

- Develop investigation processes
- None of these

Notes

-

5. How do you defend against emerging security threats?

Answered

Selected choices

- Keep up to date with security best practices
- Keep up to date with security threats
- Evaluate new security services and features regularly
- Implement new security services and features

Not selected choices

- Keep up to date with organizational, legal, and compliance requirements
- Define and prioritize risks using a threat model
- None of these

Notes

-

6. How do you protect your networks?

Answered

Selected choices

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

Not selected choices

- None of these

Notes

-

7. How do you protect your compute resources?

Answered

Selected choices

- Scan for and patch vulnerabilities
- Automate configuration management
- Automate compute protection
- Reduce attack surface
- Implement managed services

Not selected choices

- Define compute protection requirements
- None of these

Notes

-

8. How do you classify your data?

Answered

Selected choices

- Define data classification requirements
- Identify the types of data

Not selected choices

- Define data protection controls
- Implement data identification
- Automate identification and classification
- None of these

Notes

Add macie to automate "Implement data identification" & "Automate identification and classification"

9. How do you protect your data at rest?

Answered

Selected choices

- Implement secure key management
- Enforce encryption at rest
- Enforce access control

Not selected choices

- Define data management and protection at rest requirements
- Provide mechanisms to keep people away from data
- None of these

Notes

-

10. How do you protect your data in transit?

Answered

Selected choices

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

Not selected choices

- Automate detection of data leak
- None of these

Notes

-

11. How do you respond to an incident?

Answered

Selected choices

- Automate containment capability

Not selected choices

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

Notes

-

Reliability

Pillar status

Answered

Question status

Answered: 9

Not Applicable: 0

Unanswered: 0

Pillar notes

-

1. How do you manage service limits?

Answered

Selected choices

- None of these

Not selected choices

- Aware of limits but not tracking them
- Monitor and manage limits
- Use automated monitoring and management of limits
- Accommodate fixed service limits through architecture
- 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

Notes

-

2. How do you manage your network topology?

Answered

Selected choices

- Ensure IP subnet allocation accounts for expansion and availability

Not selected choices

- 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
- None of these

Notes

-

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

Answered

Selected choices

- Procure resources automatically when scaling a workload up or down

Not selected choices

- Procure resources upon detection of lack of service within a workload
- Procure resources manually upon detection that more resources may be needed soon for a workload
- Load test the workload
- None of these

Notes

-

4. How do you monitor your resources?

Answered

Selected choices

- Monitor the workload in all tiers

Not selected choices

- Send notifications based on the monitoring
- Perform automated responses on events
- Conduct reviews regularly
- None of these

Notes

-

5. How do you implement change?

Answered

Selected choices

- Deploy changes with automation

Not selected choices

- Deploy changes in a planned manner
- None of these

Notes

-

6. How do you back up data?

Answered

Selected choices

- Identify all data that needs to be backed up and are perform backups or reproduce the data from sources
- Perform data backup automatically or reproduce the data from sources automatically
- Secure and encrypt backups or ensure the data is available from a secure source for reproduction

Not selected choices

- Perform periodic recovery of the data to verify backup integrity and processes
- None of these

Notes

-

7. How does your system withstand component failures?

Answered

Selected choices

- Automate healing on all layers

Not selected choices

- 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
- Send notifications upon availability impacting events
- None of these

Notes

-

8. How do you test resilience?

Answered

Selected choices

- Inject failures to test resiliency

Not selected choices

- Use playbooks for unanticipated failures
- Conduct root cause analysis (RCA) and share results
- Conduct game days regularly
- None of these

Notes

-

9. How do you plan for disaster recovery?

Answered

Selected choices

- None of these

Not selected choices

- 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 on all changes
- Automate recovery

Notes

-

Performance Efficiency

Pillar status

Answered

Question status

Answered: 8

Not Applicable: 0

Unanswered: 0

Pillar notes

-

1. How do you select the best performing architecture?

Answered

Selected choices

- Benchmark existing workloads

Not selected choices

- 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
- Load test your workload
- None of these

Notes

-

2. How do you select your compute solution?

Answered

Selected choices

- Evaluate the available compute options
- Understand the available compute configuration options
- Collect compute-related metrics

Not selected choices

- Determine the required configuration by right-sizing
- Use the available elasticity of resources
- Re-evaluate compute needs based on metrics
- None of these

Notes

-

3. How do you select your storage solution?

Answered

Selected choices

- Understand storage characteristics and requirements
- Evaluate available configuration options

Not selected choices

- Make decisions based on access patterns and metrics
- None of these

Notes

-

4. How do you select your database solution?

Answered

Selected choices

- Understand data characteristics
- Evaluate the available options
- Collect and record database performance metrics
- Choose data storage based on access patterns

Not selected choices

- Optimize data storage based on access patterns and metrics
- None of these

Notes

-

5. How do you configure your networking solution?

Answered

Selected choices

- Understand how networking impacts performance
- Understand available product options
- Evaluate available networking features
- Use minimal network ACLs
- Leverage encryption offloading and load-balancing
- Choose network protocols to improve performance
- Choose location based on network requirements

Not selected choices

- Optimize network configuration based on metrics
- None of these

Notes

-

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

Answered

Selected choices

- Keep up-to date on new resources and services
- Evolve workload performance over time

Not selected choices

- Define a process to improve workload performance
- None of these

Notes

-

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

Answered

Selected choices

- Record performance-related metrics
- Analyze metrics when events or incidents occur
- Establish KPIs to measure workload performance
- Review metrics at regular intervals

Not selected choices

- Use monitoring to generate alarm-based notifications
- Monitor and alarm proactively
- None of these

Notes

-

8. How do you use tradeoffs to improve performance?

Answered

Selected choices

- Understand the areas where performance is most critical
- Learn about design patterns and services

Not selected choices

- Identify how tradeoffs impact customers and efficiency
- Measure the impact of performance improvements
- Use various performance-related strategies
- None of these

Notes

-

Cost Optimization

Pillar status

Answered

Question status

Answered: 9

Not Applicable: 0

Unanswered: 0

Pillar notes

-

1. How do you govern usage?

Answered

Selected choices

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

Not selected choices

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

Notes

-

2. How do you monitor usage and cost?

Answered

Selected choices

- Configure AWS Cost and Usage Report
- Define and implement tagging
- Report and notify on cost optimization
- Monitor cost proactively

Not selected choices

- Identify cost attribution categories
- Establish organization metrics
- Configure billing and cost management tools
- Allocate costs based on workload metrics
- None of these

Notes

-

3. How do you decommission resources?

Answered

Selected choices

- Track resources over their life time

Not selected choices

- Implement a decommissioning process
- Decommission resources in an unplanned manner
- Decommission resources automatically
- None of these

Notes

-

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

Answered

Selected choices

- Analyze all components of this workload

Not selected choices

- Identify organization requirements for cost
- 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
- None of these

Notes

-

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

Answered

Selected choices

- Select resource type and size based on estimates
- Select resource type and size based on metrics

Not selected choices

- Perform cost modeling
- None of these

Notes

-

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

Answered

Selected choices

- None of these

Not selected choices

- Perform pricing model analysis
- Implement different pricing models, with low coverage
- Implement regions based on cost
- Implement pricing models for all components of this workload

Notes

-

7. How do you plan for data transfer charges?

Answered

Selected choices

- None of these

Not selected choices

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

Notes

-

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

Answered

Selected choices

- Perform an analysis on the workload demand
- Provision resources reactively or unplanned
- Provision resources dynamically

Not selected choices

- None of these

Notes

-

9. How do you evaluate new services?

Answered

Selected choices

- Review and implement services in an unplanned way
- Keep up to date with new service releases

Not selected choices

- Establish a cost optimization function
- Develop a workload review process
- Review and analyze this workload regularly
- None of these

Notes

-