CCL AWS WAFR

Date Prepared:

15 March 2024

Prepared For:

Customer\_Name

# Contents

[Contents 2](#_Toc160543665)

[1.0 Introduction 4](#_Toc160543666)

[2.0 Approach 6](#_Toc160543667)

[3.0 Review 7](#_Toc160543668)

[WAFR Questionnaire 8](#_Toc160543669)

[High Risk Items (Filtered View) 24](#_Toc160543670)

[Medium Risk Items (Filtered View) 27](#_Toc160543671)

[4.0 Remediation 29](#_Toc160543672)

[5.0 Conclusion 33](#_Toc160543673)

Statement of Confidentiality

The following materials contain confidential and proprietary business information belonging to CCL. These materials may only be printed or photocopied with approval of CCL and are not to be shared with any other parties without permission.

Document Control

Document Owner

|  |  |
| --- | --- |
| Name | Position |
| Andre Bezuidenhout | AWS Principal Architect |

Version History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Changes/Comments |
| 0.1 | 05/03/2024 | Andre Bezuidenhout | Initial Draft |
|  |  |  |  |
|  |  |  |  |

Document Approvers

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Person | Position | Signature | Date |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Document Reviewers

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Person | Position | Signature | Date |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Associated Documents

|  |  |
| --- | --- |
| Document | Description/Notes |
| CCL AWS WAFR – Workshop Guide.ppt | Copy of the WAFR Workshop deck for reference |
|  |  |
|  |  |

Terms and Definitions

|  |  |
| --- | --- |
| Term | Definition |
| WAFR | Well-Architected Framework Review |

## Introduction

#### Purpose

This report details the outputs of a Well-Architected Framework Review performed for AgResearch. The review is applied to a specific candidate workload described as ServiceNow Integration workload, as part of a migration programme.

#### Background

The modern business landscape is defined by ever evolving technologies, and pressure to adapt quickly with resulting dynamic business needs. With a massive focus on cloud adoption as a solution framework, businesses are looking to realise value from their existing or future cloud investments. Thus, aligning with industry best practices to ensure optimisation across a broad spectrum of maturity pillars is critical in securing digital success in the cloud.

Public Cloud providers, such as AWS, have condensed decades worth of experience across thousands of customers to compile a set of best practices, design principles and key concepts, collectively known as the AWS Well-Architected Framework. This framework captures an evaluation of maturity and compliance across 6 pillars. These best practices are derived from the AWS Well-Architected Framework and adapted towards the specific architectures developed for Landing Zones.

**The 6 Pillars:**

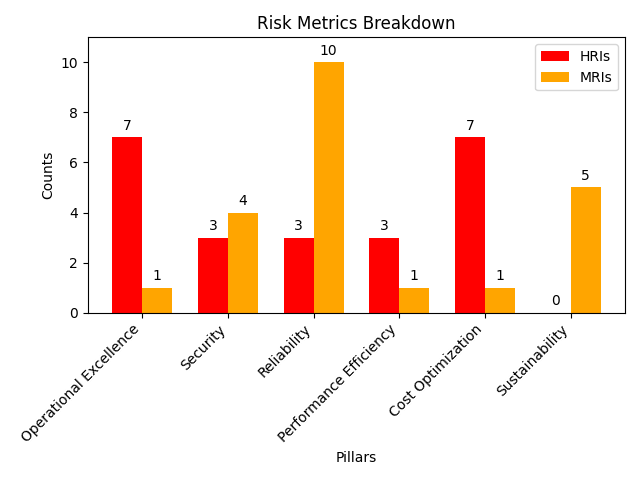
* Operational Excellence
* Security
* Reliability
* Performance Efficiency
* Cost Optimisation
* Sustainability

In addition to the standard WAFR, tailored sets of best practices have been developed into Lenses which can be applied to these 6 pillars. These lenses are specific to common workload types and industries i.e. SaaS Lens, Healthcare Lens. In this case, no additional lenses are applied for this review.

## WAFR Report

# Risk Breakdown by Pillar

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Unanswered** | **High** | **Medium** | **Not Applicable** |
| Operational Excellence | 0 | 7 | 1 | 0 |
| Security | 0 | 3 | 4 | 0 |
| Reliability | 0 | 3 | 10 | 0 |
| Performance Efficiency | 0 | 3 | 1 | 0 |
| Cost Optimization | 0 | 7 | 1 | 0 |
| Sustainability | 0 | 0 | 5 | 0 |



# High Risk Items

|  |  |  |
| --- | --- | --- |
| **Pillar Name** | **Question Title** | **Best Practice Choice** |
| Operational Excellence | OPS 2. How do you structure your organization to support your business outcomes? | Mechanisms exist to identify responsibility and ownership |
| Mechanisms exist to request additions, changes, and exceptions |
| Responsibilities between teams are predefined or negotiated |
| Operational Excellence | OPS 3. How does your organizational culture support your business outcomes? | Communications are timely, clear, and actionable |
| Experimentation is encouraged |
| Resource teams appropriately |
| Operational Excellence | OPS 4. How do you design your workload so that you can understand its state? | Implement application telemetry |
| Implement and configure workload telemetry |
| Implement user activity telemetry |
| Implement dependency telemetry |
| Implement transaction traceability |
| Operational Excellence | OPS 5. How do you reduce defects, ease remediation, and improve flow into production? | 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 |
| Operational Excellence | OPS 8. How do you understand the health of your workload? | 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 |
| Operational Excellence | OPS 9. How do you understand the health of your operations? | 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 |
| Operational Excellence | OPS 10. How do you manage workload and operations events? | Use a process for event, incident, and problem management |
| Have a process per alert |
| Prioritize operational events based on business impact |
| Automate responses to events |
| Security | SEC 1. How do you securely operate your workload? | Identify threats and prioritize mitigations using a threat model |
| Security | SEC 6. How do you protect your compute resources? | Perform vulnerability management |
| Reduce attack surface |
| Implement managed services |
| Reliability | REL 3. How do you design your workload service architecture? | Choose how to segment your workload |
| Provide service contracts per API |
| Reliability | REL 4. How do you design interactions in a distributed system to prevent failures? | Identify which kind of distributed system is required |
| Implement loosely coupled dependencies |
| Make all responses idempotent |
| Do constant work |
| Reliability | REL 5. How do you design interactions in a distributed system to mitigate or withstand failures? | 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 |
| Performance Efficiency | PERF 2. How do you select your compute solution? | Evaluate the available compute options |
| Understand the available compute configuration options |
| Performance Efficiency | PERF 4. How do you select your database solution? | Collect and record database performance metrics |
| Choose data storage based on access patterns |
| Performance Efficiency | PERF 5. How do you configure your networking solution? | Understand how networking impacts performance |
| Choose network protocols to improve performance |
| Choose your workload’s location based on network requirements |
| Cost Optimisation | COST 2. How do you govern usage? | Develop policies based on your organization requirements |
| Cost Optimisation | COST 3. How do you monitor usage and cost? | Identify cost attribution categories |
| Establish organization metrics |
| Add organization information to cost and usage |
| Allocate costs based on workload metrics |
| Cost Optimisation | COST 5. How do you evaluate cost when you select services? | 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 in line with organization priorities |
| Perform cost analysis for different usage over time |
| Select software with cost effective licensing |
| Cost Optimisation | COST 6. How do you meet cost targets when you select resource type, size and number? | Perform cost modeling |
| Select resource type, size, and number based on data |
| Select resource type, size, and number automatically based on metrics |
| Cost Optimisation | COST 7. How do you use pricing models to reduce cost? | 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 |
| Cost Optimisation | COST 8. How do you plan for data transfer charges? | Perform data transfer modeling |
| Select components to optimize data transfer cost |
| Implement services to reduce data transfer costs |
| Cost Optimisation | COST 9. How do you manage demand, and supply resources? | Perform an analysis on the workload demand |
| Implement a buffer or throttle to manage demand |
| Supply resources dynamically |

# Medium Risk Items

|  |  |  |
| --- | --- | --- |
| **Pillar Name** | **Question Title** | **Best Practice Choice** |
| Security | SEC 5. How do you protect your network resources? | Automate network protection |
| Implement inspection and protection |
| Security | SEC 7. How do you classify your data? | Automate identification and classification |
| Security | SEC 8. How do you protect your data at rest? | Automate data at rest protection |
| Security | SEC 9. How do you protect your data in transit? | Automate detection of unintended data  access |
| Authenticate network communications |
| Reliability | REL 1. How do you manage service quotas and constraints? | Automate quota management |
| Ensure that a sufficient gap exists between the current quotas and the maximum usage to accommodate failover |
| Reliability | REL 2. How do you plan your network topology? | Prefer hub-and-spoke topologies over many-to-many mesh |
| Reliability | REL 6. How do you monitor workload resources? | Analytics |
| Conduct reviews regularly |
| Monitor end-to-end tracing of requests through your system |
| Reliability | REL 7. How do you design your workload to adapt to changes in demand? | Load test your workload |
| Reliability | REL 8. How do you implement change? | Integrate resiliency testing as part of your deployment |
| Deploy using immutable infrastructure |
| Deploy changes with automation |
| Reliability | REL 9. How do you back up data? | Perform periodic recovery of the data to verify backup integrity and processes |
| Reliability | REL 10. How do you use fault isolation to protect your workload? | Use bulkhead architectures to limit scope of impact |
| Automate recovery for components constrained to a single location |
| Performance Efficiency | PERF 6. How do you evolve your workload to take advantage of new releases? | Define a process to improve workload performance |
| Cost Optimisation | COST 4. How do you decommission resources? | Enforce data retention policies |
| Sustainability | SUS 1. How do you select Regions for your workload? | Choose Region based on both business requirements and sustainability goals |
| Sustainability | SUS 3. How do you take advantage of software and architecture patterns to support your Sustainability goals? | Optimize software and architecture for asynchronous and scheduled jobs |
| Remove or refactor workload components with low or no use |
| Optimize areas of code that consume the most time or resources |
| Optimize impact on devices and equipment |
| Use software patterns and architectures that best support data access and storage patterns |
| Sustainability | SUS 4. How do you take advantage of data management policies and patterns to support your Sustainability goals? | Use elasticity and automation to expand block storage or file system |
| Back up data only when difficult to recreate |
| Sustainability | SUS 5. How do you select and use cloud hardware and services in your architecture to support your Sustainability goals? | Use managed services |
| Sustainability | SUS 6. How do your organizational processes support your Sustainability goals? | Adopt methods that can rapidly introduce sustainability improvements |
| Increase utilization of build environments |
| Use managed device farms for testing |

## Remediation Plan

### Quick Wins

|  |  |  |
| --- | --- | --- |
| **#** | **Question** | **Best Practice** |
| 1 | OPS 2. How do you structure your organization to support your business outcomes? | Mechanisms exist to identify responsibility and ownership |
| 2 | OPS 2. How do you structure your organization to support your business outcomes? | Mechanisms exist to request additions, changes, and exceptions |
| 3 | OPS 2. How do you structure your organization to support your business outcomes? | Responsibilities between teams are predefined or negotiated |
| 4 | OPS 3. How does your organizational culture support your business outcomes? | Communications are timely, clear, and actionable |
| 5 | OPS 3. How does your organizational culture support your business outcomes? | Experimentation is encouraged |
| 6 | OPS 3. How does your organizational culture support your business outcomes? | Resource teams appropriately |
| 7 | SEC 1. How do you securely operate your workload? | Identify threats and prioritize mitigations using a threat model |
| 8 | SEC 6. How do you protect your compute resources? | Perform vulnerability management |
| 9 | SEC 6. How do you protect your compute resources? | Reduce attack surface |
| 10 | SEC 6. How do you protect your compute resources? | Implement managed services |

#### Mechanisms exist to identify responsibility and ownership

##### Description

Implement a process to clearly define ownership and responsibilities for key business and technical roles.

##### Remediation

A RACI (Responsible, Accountable, Consulted, Informed) matrix should be created mapping business and technical roles to key processes and assets. This will identify clear owners responsible for each area. Regular attestations should be performed to keep this matrix up to date.

##### Additional Considerations

Consider automating the attestation process through a workflow in a CMDB system. Make sure to communicate changes in ownership clearly across the organization.

##### Effort Estimate

2 weeks for initial matrix definition and implementation of attestation workflow

##### Resourcing and Skills

Program manager, process engineer

##### Domain Impact

Operations

#### Mechanisms exist to request additions, changes, and exceptions

##### Description

Implement a process for users to request changes or exceptions to configurations

##### Remediation

Create a self-service portal where users can submit requests for changes or exceptions. Have an approval workflow before changes are implemented. Log all requests and approvals.

##### Additional Considerations

Ensure proper access controls on the portal. Requests should link to tickets or other tracking mechanisms.

##### Effort Estimate

2 weeks development time plus ongoing operational overhead

##### Resourcing and Skills

Frontend developer, security architect

##### Domain Impact

Operations, Security

#### Responsibilities between teams are predefined or negotiated

##### Description

Define clear responsibilities between teams to support business outcomes

##### Remediation

Have leadership facilitate sessions with teams to predefine responsibilities based on organizational structure, or have teams negotiate responsibilities between themselves based on project needs.

##### Additional Considerations

Ensure there is accountability for owning responsibilities, and a process for negotiating changes when needed.

##### Effort Estimate

2 week effort: Week 1 - Facilitate sessions to define team responsibilities. Week 2 - Document decisions and communicate expectations.

##### Resourcing and Skills

Leadership, key stakeholders from teams

##### Domain Impact

Operations, Productivity

#### Communications are timely, clear, and actionable

##### Description

Improve organizational communications to be more timely, clear, and actionable

##### Remediation

Conduct an assessment of current communication practices and channels. Identify areas for improvement around timeliness, clarity, and ability to drive action based on the communications. Develop updated practices, channels, and example communications to address the gaps.

##### Additional Considerations

Ensure two-way communication channels to enable clarifying questions and feedback. Use simple language and avoid complex technical terms when possible.

##### Effort Estimate

2 weeks - Assessment of current practices (1 week), Development of updated practices and examples (1 week)

##### Resourcing and Skills

Communications lead, Sample audiences for updated practices

##### Domain Impact

Operations, Security

#### Experimentation is encouraged

##### Description

Encourage experimentation by implementing mechanisms to test new ideas with low risk

##### Remediation

Form a small team to brainstorm experimental projects. Start with low-risk, low-effort experiments. Publicize successful results across the organization. Consider an innovation budget and contest to fund promising experiments.

##### Additional Considerations

Experiments should align to business goals and outcomes. Balance experimentation with focus and execution.

##### Effort Estimate

Set up innovation team: 2 weeks. Run first round of experiments: 4 weeks. Continual improvement effort.

##### Resourcing and Skills

Innovation team. Potential budget for experiments.

##### Domain Impact

Culture, Product/Service Innovation

#### Resource teams appropriately

##### Description

Ensure teams are resourced appropriately to support business outcomes

##### Remediation

Conduct an assessment of current team resourcing and workloads. Identify gaps where teams are under-resourced. Develop a hiring plan to bring on additional headcount and allow teams to focus on critical outcomes.

##### Additional Considerations

When resourcing teams, consider broader organizational goals beyond the scope of specific teams. Pursue cross-training and resource sharing opportunities across teams where appropriate.

##### Effort Estimate

2-4 weeks to conduct assessment and develop hiring plan. 4-8 weeks to onboard new hires.

##### Resourcing and Skills

HR business partner, finance partner, team managers

##### Domain Impact

Operations, Human Resources

#### Identify threats and prioritize mitigations using a threat model

##### Description

Perform a threat modeling exercise to identify potential threats and vulnerabilities for the workload. Prioritize mitigations based on risk and impact.

##### Remediation

Gather architects, security experts, and developers to create a threat model using a framework like STRIDE or PASTA. Document components, data flows, trust boundaries, entry/exit points. Identify threats like data exfiltration, DoS, account compromise. Prioritize threats based on likelihood and impact. Determine risk mitigation solutions for high priority threats.

##### Additional Considerations

Consider integrating threat modeling early in the SDLC. Revisit the threat model periodically and after major architecture changes. Leverage available AWS resources like Well-Architected reviews.

##### Effort Estimate

2 weeks for initial threat modeling exercise. 1 week for implementation of critical security controls.

##### Resourcing and Skills

Security architects, Risk/Compliance roles, Developers

##### Domain Impact

Security

#### Perform vulnerability management

##### Description

Implement a vulnerability management program to continuously monitor compute resources for vulnerabilities and misconfigurations.

##### Remediation

Enable Amazon Inspector to run vulnerability scans on EC2 instances on a regular cadence. Analyze findings and implement fixes and mitigate risks based on criticality. Consider tools like Qualys or Rapid7 to complement Inspector capabilities.

##### Additional Considerations

Have a well defined process for tracking, prioritizing and fixing vulnerabilities discovered during scans. Integrate scanning into CI/CD pipelines.

##### Effort Estimate

2 weeks for implementation; ongoing effort for continuous scans and remediations

##### Resourcing and Skills

Security engineer, operations engineer

##### Domain Impact

Security

#### Reduce attack surface

##### Description

Reduce the attack surface of compute resources by removing unnecessary ports, protocols, services, credentials, and permissions.

##### Remediation

Review compute instance configurations and security groups to identify unnecessary open ports, protocols, services running, credentials stored, and permissions granted. Create a remediation plan to close ports, disable unused services, rotate credentials, and apply the principle of least privilege to permissions.

##### Additional Considerations

When reducing attack surface, carefully test changes in staging environments before deploying to production to avoid availability issues. Monitor systems post-deployment to ensure no loss of critical functionality.

##### Effort Estimate

2 weeks - Review configurations and create remediation plan; 4 weeks - Execute staged deployments of changes across estate

##### Resourcing and Skills

Security analyst, Infrastructure engineer

##### Domain Impact

Security

#### Implement managed services

##### Description

Enable AWS managed services like AWS Config and AWS Security Hub to continuously monitor your environment, detect misconfigurations, and identify vulnerabilities.

##### Remediation

1. Enable AWS Config to continuously monitor and record your AWS resource configurations. Review Config rules and ensure critical best practices are being checked.  
2. Enable AWS Security Hub which aggregates and prioritizes security alerts and findings from multiple AWS services. Customize Security Hub with additional security checks as needed.  
3. Consider AWS managed services like Systems Manager and Inspector to further enhance visibility and security of your compute resources.

##### Additional Considerations

When enabling AWS managed services, carefully review service scopes, access permissions, and costs to ensure proper governance controls are in place.

##### Effort Estimate

Quick win - Enable AWS Config and Security Hub via AWS Console or CloudFormation templates. Takes less than 1 day.

##### Resourcing and Skills

AWS Cloud Operations or Security team to configure services. CloudFormation expertise helpful but not required.

##### Domain Impact

Security