CCL AWS WAFR

Date Prepared:

5 March 2024

Prepared For:

AgResearch

# 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.

#### Scope and Deliverables

This report covers the review of a Landing Zone only, where it is currently hosted on AWS with the intent of optimising in AWS.

The following AWS WAFR Lenses have been applied:

* **N/A**

The following AWS WAFR Pillars have been covered:

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

**In-scope Deliverables**

* AWS WAFR Questionnaire and Responses
* Risk item breakdown (High Risk Items, Medium Risk Items)
* AWS WAFR Pillar Summaries
* Remediation Mapping and Prioritisation

**Out-of-scope Deliverables**

* Deployment of tools/agents for data collection

#### Key Contact Details

The following people are the intended key Client and CCL recipients for any notifications or first point of contact regarding the SOW. If any details change during the period of work, the relevant party will promptly notify the other.

|  |  |  |  |
| --- | --- | --- | --- |
| Client Contact Details | | CCL Contact Details | |
| Contact Name |  | Contact Name | Leeanda Keomany |
| Title |  | Title | Head of Delivery & Capability |
| Address |  | Address | 15 Willeston St, Wellington |
| Phone Number |  | Phone Number | +64 21 226 9985 |
| Email |  | Email | Leeanda.keomany@concepts.co.nz |

## Approach

CCL, being an accredited and accepted AWS Well-Architected Partner, follows the official review process as prescribed by AWS, where applicable. Due to the nature of this requirement being bespoke, and focused on the review of a **ServiceNow Integration Workload**, CCL processes and outputs will be used exclusively. Note that these processes and tools are designed in alignment with official AWS WAFR lenses.

* Workload architecture diagram analysis/review
* 6-Pillar AWS WAFR workshop/interviews with workload solution stakeholders
* Lens workshop/interviews (not applicable)
* Data capturing using CCL Questionnaires
* Risk and Remediation derivations from AWS WAFR best practices
* CCL Solution mapping in alignment with identified remediation/improvement plans
* Presentation of this report document.

Note, this report is to be treated within the context of a review, and not an audit.

## Review

#### CCL Landing Zone Lens

###### Review Summary

|  |  |  |  |
| --- | --- | --- | --- |
| Pillar | Questions Answered | High Risk | Medium Risk |
| Operational Excellence | 11/11 | 3 | 4 |
| Security | 11/11 | 2 | 2 |
| Reliability | 13/13 | 6 | 3 |
| Performance | 5/5 | 2 | 1 |
| Cost Optimisation | 11/11 | 3 | 2 |
| Sustainability | 6/6 | 0 | 0 |
| **TOTAL** | **57/57** | **16** | **12** |

# WAFR Questionnaire

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Pillar Name** | **Question** | **BP #** | **Choice (Best Practice)** | **Y/N** |
| Cost Optimization | How do you implement cloud financial management? | BP\_1 | Establish cloud budgets and forecasts | Y |
| BP\_2 | Implement cost awareness in your organizational processes | Y |
| BP\_3 | Create a cost-aware culture | Y |
| BP\_4 | Establish ownership of cost optimization | N |
| BP\_5 | Establish a partnership between finance and technology | Y |
| BP\_6 | Monitor cost proactively | Y |
| BP\_7 | Quantify business value from cost optimization | Y |
| BP\_8 | Keep up-to-date with new service releases | Y |
| BP\_9 | Report and notify on cost optimization | Y |
| Cost Optimization | How do you plan for data transfer charges? | BP\_10 | Implement services to reduce data transfer costs | N |
| BP\_11 | Perform data transfer modeling | N |
| BP\_12 | Select components to optimize data transfer cost | N |
| Cost Optimization | How do you decommission resources? | BP\_13 | Enforce data retention policies | Y |
| BP\_14 | Decommission resources automatically | N |
| BP\_15 | Decommission resources | Y |
| BP\_16 | Implement a decommissioning process | N |
| BP\_17 | Track resources over their life time | Y |
| Cost Optimization | How do you evaluate the cost of effort? | BP\_18 | Perform automation for operations | N |
| Cost Optimization | How do you evaluate new services? | BP\_19 | Develop a workload review process | N |
| BP\_20 | Review and analyze this workload regularly | N |
| Cost Optimization | How do you govern usage? | BP\_21 | Implement an account structure | Y |
| BP\_22 | Implement cost controls | Y |
| BP\_23 | Implement goals and targets | Y |
| BP\_24 | Implement groups and roles | Y |
| BP\_25 | Develop policies based on your organization requirements | Y |
| BP\_26 | Track project lifecycle | Y |
| Cost Optimization | How do you manage demand, and supply resources? | BP\_27 | Implement a buffer or throttle to manage demand | N |
| BP\_28 | Perform an analysis on the workload demand | Y |
| BP\_29 | Supply resources dynamically | N |
| Cost Optimization | How do you monitor your cost and usage? | BP\_30 | Allocate costs based on workload metrics | N |
| BP\_31 | Configure billing and cost management tools | Y |
| BP\_32 | Identify cost attribution categories | N |
| BP\_33 | Establish organization metrics | N |
| BP\_34 | Configure detailed information sources | N |
| BP\_35 | Add organization information to cost and usage | N |
| Cost Optimization | How do you use pricing models to reduce cost? | BP\_36 | Perform pricing model analysis | Y |
| BP\_37 | Implement pricing models for all components of this workload | Y |
| BP\_38 | Perform pricing model analysis at the management account level | Y |
| BP\_39 | Choose Regions based on cost | N |
| BP\_40 | Select third-party agreements with cost-efficient terms | N |
| Cost Optimization | How do you evaluate cost when you select services? | BP\_41 | Analyze all components of this workload | Y |
| BP\_42 | Perform cost analysis for different usage over time | N |
| BP\_43 | Select software with cost effective licensing | Y |
| BP\_44 | Identify organization requirements for cost | Y |
| BP\_45 | Select components of this workload to optimize cost in line with organization priorities | Y |
| BP\_46 | Perform a thorough analysis of each component | Y |
| Cost Optimization | How do you meet cost targets when you select resource type, size and number? | BP\_47 | Perform cost modeling | Y |
| BP\_48 | Select resource type, size, and number based on data | Y |
| BP\_49 | Select resource type, size, and number automatically based on metrics | N |
| Operational Excellence | How do you reduce defects, ease remediation, and improve flow into production? | BP\_50 | Fully automate integration and deployment | Y |
| BP\_51 | Use build and deployment management systems | Y |
| BP\_52 | Implement practices to improve code quality | N |
| BP\_53 | Use configuration management systems | Y |
| BP\_54 | Make frequent, small, reversible changes | Y |
| BP\_55 | Use multiple environments | Y |
| BP\_56 | Perform patch management | Y |
| BP\_57 | Share design standards | N |
| BP\_58 | Test and validate changes | Y |
| BP\_59 | Use version control | Y |
| Operational Excellence | How do you manage workload and operations events? | BP\_60 | Automate responses to events | N |
| BP\_61 | Communicate status through dashboards | Y |
| BP\_62 | Define escalation paths | Y |
| BP\_63 | Use a process for event, incident, and problem management | Y |
| BP\_64 | Prioritize operational events based on business impact | Y |
| BP\_65 | Have a process per alert | Y |
| BP\_66 | Define a customer communication plan for outages | Y |
| Operational Excellence | How do you evolve operations? | BP\_67 | Allocate time to make improvements | Y |
| BP\_68 | Define drivers for improvement | Y |
| BP\_69 | Implement feedback loops | N |
| BP\_70 | Perform knowledge management | Y |
| BP\_71 | Perform operations metrics reviews | N |
| BP\_72 | Perform post-incident analysis | Y |
| BP\_73 | Have a process for continuous improvement | Y |
| BP\_74 | Document and share lessons learned | Y |
| BP\_75 | Validate insights | Y |
| Operational Excellence | How do you mitigate deployment risks? | BP\_76 | Automate testing and rollback | Y |
| BP\_77 | Employ safe deployment strategies | Y |
| BP\_78 | Plan for unsuccessful changes | Y |
| BP\_79 | Test deployments | Y |
| Operational Excellence | How do you implement observability in your workload? | BP\_80 | Implement application telemetry | Y |
| BP\_81 | Implement user experience telemetry | N |
| BP\_82 | Implement dependency telemetry | N |
| BP\_83 | Implement distributed tracing | N |
| BP\_84 | Identify key performance indicators | N |
| Operational Excellence | How do you understand the health of your operations? | BP\_85 | Communicate status and trends to ensure visibility into operation | N |
| BP\_86 | Measure operations goals and KPIs with metrics | Y |
| BP\_87 | Review operations metrics and prioritize improvement | N |
| Operational Excellence | How do you structure your organization to support your business outcomes? | BP\_88 | Operations activities have identified owners responsible for their performance | Y |
| BP\_89 | Responsibilities between teams are predefined or negotiated | Y |
| BP\_90 | Processes and procedures have identified owners | Y |
| BP\_91 | Resources have identified owners | Y |
| BP\_92 | Mechanisms exist to identify responsibility and ownership | Y |
| BP\_93 | Team members know what they are responsible for | Y |
| BP\_94 | Mechanisms exist to request additions, changes, and exceptions | Y |
| Operational Excellence | How does your organizational culture support your business outcomes? | BP\_95 | Diverse opinions are encouraged and sought within and across teams | Y |
| BP\_96 | Communications are timely, clear, and actionable | Y |
| BP\_97 | Executive Sponsorship | Y |
| BP\_98 | Team members are empowered to take action when outcomes are at risk | Y |
| BP\_99 | Escalation is encouraged | Y |
| BP\_100 | Experimentation is encouraged | Y |
| BP\_101 | Team members are encouraged to maintain and grow their skill sets | Y |
| BP\_102 | Resource teams appropriately | N |
| Operational Excellence | How do you determine what your priorities are? | BP\_103 | Evaluate compliance requirements | Y |
| BP\_104 | Evaluate threat landscape | Y |
| BP\_105 | Evaluate tradeoffs | Y |
| BP\_106 | Evaluate external customer needs | Y |
| BP\_107 | Evaluate governance requirements | Y |
| BP\_108 | Evaluate internal customer needs | Y |
| BP\_109 | Manage benefits and risks | Y |
| Operational Excellence | How do you know that you are ready to support a workload? | BP\_110 | Ensure a consistent review of operational readiness | Y |
| BP\_111 | Create support plans for production workloads | Y |
| BP\_112 | Make informed decisions to deploy systems and changes | Y |
| BP\_113 | Ensure personnel capability | N |
| BP\_114 | Use playbooks to investigate issues | N |
| BP\_115 | Use runbooks to perform procedures | N |
| Operational Excellence | How do you utilize workload observability in your organization? | BP\_116 | Analyze workload logs | N |
| BP\_117 | Analyze workload metrics | Y |
| BP\_118 | Analyze workload traces | N |
| BP\_119 | Create actionable alerts | Y |
| BP\_120 | Create dashboards | N |
| Performance Efficiency | How do you select and use compute resources in your workload? | BP\_121 | Collect compute-related metrics | Y |
| BP\_122 | Use optimized hardware-based compute accelerators | N |
| BP\_123 | Configure and right-size compute resources | Y |
| BP\_124 | Scale your compute resources dynamically | N |
| BP\_125 | Select the best compute options for your workload | Y |
| BP\_126 | Understand the available compute configuration and features | Y |
| Performance Efficiency | How do you store, manage, and access data in your workload? | BP\_127 | Implement data access patterns that utilize caching | N |
| BP\_128 | Collect and record data store performance metrics | Y |
| BP\_129 | Evaluate available configuration options for data store | Y |
| BP\_130 | Implement strategies to improve query performance in data store | N |
| BP\_131 | Use purpose-built data store that best support your data access and storage requirements | Y |
| Performance Efficiency | How do you select and configure networking resources in your workload? | BP\_132 | Choose appropriate dedicated connectivity or VPN for your workload | Y |
| BP\_133 | Choose network protocols to improve performance | Y |
| BP\_134 | Choose your workload's location based on network requirements | Y |
| BP\_135 | Evaluate available networking features | N |
| BP\_136 | Use load balancing to distribute traffic across multiple resources | N |
| BP\_137 | Optimize network configuration based on metrics | Y |
| BP\_138 | Understand how networking impacts performance | Y |
| Performance Efficiency | How do you select the appropriate cloud resources and architecture patterns for your workload? | BP\_139 | Evaluate how trade-offs impact customers and architecture efficiency | Y |
| BP\_140 | Factor cost into architectural decisions | Y |
| BP\_141 | Use guidance from your cloud provider or an appropriate partner to learn about architecture patterns and best practices | Y |
| BP\_142 | Learn about and understand available cloud services and features | Y |
| BP\_143 | Use benchmarking to drive architectural decisions | N |
| BP\_144 | Use a data-driven approach for architectural choices | Y |
| BP\_145 | Use policies and reference architectures | Y |
| Performance Efficiency | What process do you use to support more performance efficiency for your workload? | BP\_146 | Use automation to proactively remediate performance-related issues | N |
| BP\_147 | Establish key performance indicators (KPIs) to measure workload health and performance | Y |
| BP\_148 | Keep your workload and services up-to-date | Y |
| BP\_149 | Load test your workload | Y |
| BP\_150 | Review metrics at regular intervals | Y |
| BP\_151 | Use monitoring solutions to understand the areas where performance is most critical | Y |
| BP\_152 | Define a process to improve workload performance | N |
| Reliability | How do you design your workload to adapt to changes in demand? | BP\_153 | Use automation when obtaining or scaling resources | N |
| BP\_154 | Load test your workload | N |
| BP\_155 | Obtain resources upon detection that more resources are needed for a workload | N |
| BP\_156 | Obtain resources upon detection of impairment to a workload | N |
| Reliability | How do you back up data? | BP\_157 | Perform data backup automatically | Y |
| BP\_158 | Identify and back up all data that needs to be backed up, or reproduce the data from sources | Y |
| BP\_159 | Perform periodic recovery of the data to verify backup integrity and processes | Y |
| BP\_160 | Secure and encrypt backups | Y |
| Reliability | How do you use fault isolation to protect your workload? | BP\_161 | Deploy the workload to multiple locations | N |
| BP\_162 | Select the appropriate locations for your multi-location deployment | N |
| BP\_163 | Automate recovery for components constrained to a single location | N |
| BP\_164 | Use bulkhead architectures to limit scope of impact | N |
| Reliability | How do you manage service quotas and constraints? | BP\_165 | Automate quota management | N |
| BP\_166 | Accommodate fixed service quotas and constraints through architecture | N |
| BP\_167 | Aware of service quotas and constraints | N |
| BP\_168 | Manage service quotas across accounts and Regions | N |
| BP\_169 | Monitor and manage quotas | Y |
| BP\_170 | Ensure that a sufficient gap exists between the current quotas and the maximum usage to accommodate failover | N |
| Reliability | How do you design interactions in a distributed system to mitigate or withstand failures? | BP\_171 | Set client timeouts | N |
| BP\_172 | Implement emergency levers | N |
| BP\_173 | Fail fast and limit queues | N |
| BP\_174 | Implement graceful degradation to transform applicable hard dependencies into soft dependencies | N |
| BP\_175 | Control and limit retry calls | N |
| BP\_176 | Make services stateless where possible | N |
| BP\_177 | Throttle requests | N |
| Reliability | How do you monitor workload resources? | BP\_178 | Automate responses (Real-time processing and alarming) | Y |
| BP\_179 | Monitor end-to-end tracing of requests through your system | N |
| BP\_180 | Monitor all components for the workload (Generation) | Y |
| BP\_181 | Define and calculate metrics (Aggregation) | N |
| BP\_182 | Send notifications (Real-time processing and alarming) | Y |
| BP\_183 | Conduct reviews regularly | N |
| BP\_184 | Analytics | Y |
| Reliability | How do you plan for disaster recovery (DR)? | BP\_185 | Automate recovery | N |
| BP\_186 | Manage configuration drift at the DR site or Region | N |
| BP\_187 | Use defined recovery strategies to meet the recovery objectives | Y |
| BP\_188 | Test disaster recovery implementation to validate the implementation | Y |
| BP\_189 | Define recovery objectives for downtime and data loss | Y |
| Reliability | How do you plan your network topology? | BP\_190 | Provision redundant connectivity between private networks in the cloud and on-premises environments | Y |
| BP\_191 | Use highly available network connectivity for your workload public endpoints | N |
| BP\_192 | Ensure IP subnet allocation accounts for expansion and availability | Y |
| BP\_193 | Enforce non-overlapping private IP address ranges in all private address spaces where they are connected | Y |
| BP\_194 | Prefer hub-and-spoke topologies over many-to-many mesh | Y |
| Reliability | How do you design interactions in a distributed system to prevent failures? | BP\_195 | Do constant work | Y |
| BP\_196 | Make all responses idempotent | N |
| BP\_197 | Identify which kind of distributed system is required | N |
| BP\_198 | Implement loosely coupled dependencies | Y |
| Reliability | How do you design your workload service architecture? | BP\_199 | Provide service contracts per API | N |
| BP\_200 | Build services focused on specific business domains and functionality | N |
| BP\_201 | Choose how to segment your workload | Y |
| Reliability | How do you test reliability? | BP\_202 | Test resiliency using chaos engineering | N |
| BP\_203 | Conduct game days regularly | Y |
| BP\_204 | Use playbooks to investigate failures | N |
| BP\_205 | Perform post-incident analysis | Y |
| BP\_206 | Test functional requirements | Y |
| BP\_207 | Test scaling and performance requirements | Y |
| Reliability | How do you implement change? | BP\_208 | Deploy changes with automation | Y |
| BP\_209 | Integrate functional testing as part of your deployment | Y |
| BP\_210 | Deploy using immutable infrastructure | N |
| BP\_211 | Use runbooks for standard activities such as deployment | Y |
| BP\_212 | Integrate resiliency testing as part of your deployment | N |
| Reliability | How do you design your workload to withstand component failures? | BP\_213 | Automate healing on all layers | N |
| BP\_214 | Rely on the data plane and not the control plane during recovery | N |
| BP\_215 | Fail over to healthy resources | N |
| BP\_216 | Monitor all components of the workload to detect failures | Y |
| BP\_217 | Send notifications when events impact availability | Y |
| BP\_218 | Architect your product to meet availability targets and uptime service level agreements (SLAs) | N |
| BP\_219 | Use static stability to prevent bimodal behavior | N |
| Security | How do you incorporate and validate the security properties of applications throughout the design, development, and deployment lifecycle? | BP\_220 | Automate testing throughout the development and release lifecycle | N |
| BP\_221 | Build a program that embeds security ownership in workload teams | Y |
| BP\_222 | Centralize services for packages and dependencies | Y |
| BP\_223 | Deploy software programmatically | N |
| BP\_224 | Manual code reviews | N |
| BP\_225 | Perform regular penetration testing | N |
| BP\_226 | Regularly assess security properties of the pipelines | Y |
| BP\_227 | Train for application security | N |
| Security | How do you classify your data? | BP\_228 | Automate identification and classification | N |
| BP\_229 | Define data protection controls | Y |
| BP\_230 | Identify the data within your workload | N |
| BP\_231 | Define data lifecycle management | N |
| Security | How do you detect and investigate security events? | BP\_232 | Implement actionable security events | Y |
| BP\_233 | Analyze logs, findings, and metrics centrally | Y |
| BP\_234 | Configure service and application logging | Y |
| BP\_235 | Automate response to events | N |
| Security | How do you manage identities for people and machines? | BP\_236 | Audit and rotate credentials periodically | Y |
| BP\_237 | Use strong sign-in mechanisms | Y |
| BP\_238 | Leverage user groups and attributes | Y |
| BP\_239 | Rely on a centralized identity provider | Y |
| BP\_240 | Store and use secrets securely | Y |
| BP\_241 | Use temporary credentials | Y |
| Security | How do you anticipate, respond to, and recover from incidents? | BP\_242 | Develop incident management plans | Y |
| BP\_243 | Establish a framework for learning from incidents | Y |
| BP\_244 | Identify key personnel and external resources | Y |
| BP\_245 | Develop and test security incident response playbooks | Y |
| BP\_246 | Pre-deploy tools | N |
| BP\_247 | Pre-provision access | N |
| BP\_248 | Prepare forensic capabilities | N |
| BP\_249 | Run simulations | Y |
| Security | How do you protect your network resources? | BP\_250 | Automate network protection | Y |
| BP\_251 | Create network layers | Y |
| BP\_252 | Implement inspection and protection | Y |
| BP\_253 | Control traffic at all layers | Y |
| Security | How do you manage permissions for people and machines? | BP\_254 | Analyze public and cross account access | Y |
| BP\_255 | Reduce permissions continuously | Y |
| BP\_256 | Define access requirements | Y |
| BP\_257 | Define permission guardrails for your organization | Y |
| BP\_258 | Establish emergency access process | Y |
| BP\_259 | Grant least privilege access | Y |
| BP\_260 | Manage access based on life cycle | Y |
| BP\_261 | Share resources securely within your organization | Y |
| BP\_262 | Share resources securely with a third party | Y |
| Security | How do you protect your compute resources? | BP\_263 | Enable people to perform actions at a distance | Y |
| BP\_264 | Automate compute protection | Y |
| BP\_265 | Implement managed services | Y |
| BP\_266 | Reduce attack surface | Y |
| BP\_267 | Validate software integrity | Y |
| BP\_268 | Perform vulnerability management | Y |
| Security | How do you protect your data at rest? | BP\_269 | Enforce access control | Y |
| BP\_270 | Automate data at rest protection | Y |
| BP\_271 | Enforce encryption at rest | Y |
| BP\_272 | Implement secure key management | Y |
| BP\_273 | Use mechanisms to keep people away from data | Y |
| Security | How do you protect your data in transit? | BP\_274 | Authenticate network communications | Y |
| BP\_275 | Automate detection of unintended data access | Y |
| BP\_276 | Enforce encryption in transit | Y |
| BP\_277 | Implement secure key and certificate management | Y |
| Security | How do you securely operate your workload? | BP\_278 | Secure account root user and properties | Y |
| BP\_279 | Identify and validate control objectives | Y |
| BP\_280 | Evaluate and implement new security services and features regularly | Y |
| BP\_281 | Separate workloads using accounts | Y |
| BP\_282 | Automate testing and validation of security controls in pipelines | Y |
| BP\_283 | Identify and prioritize risks using a threat model | Y |
| BP\_284 | Keep up-to-date with security recommendations | Y |
| BP\_285 | Keep up-to-date with security threats | Y |
| Sustainability | How do you take advantage of data management policies and patterns to support your sustainability goals? | BP\_286 | Implement a data classification policy | Y |
| BP\_287 | Use technologies that support data access and storage patterns | Y |
| BP\_288 | Use policies to manage the lifecycle of your datasets | N |
| BP\_289 | Use elasticity and automation to expand block storage or file system | N |
| BP\_290 | Remove unneeded or redundant data | Y |
| BP\_291 | Use shared file systems or storage to access common data | N |
| BP\_292 | Minimize data movement across networks | N |
| BP\_293 | Back up data only when difficult to recreate | N |
| Sustainability | How do your organizational processes support your sustainability goals? | BP\_294 | Adopt methods that can rapidly introduce sustainability improvements | N |
| BP\_295 | Keep your workload up-to-date | N |
| BP\_296 | Increase utilization of build environments | N |
| BP\_297 | Use managed device farms for testing | N |
| Sustainability | How do you select and use cloud hardware and services in your architecture to support your sustainability goals? | BP\_298 | Use the minimum amount of hardware to meet your needs | Y |
| BP\_299 | Use instance types with the least impact | Y |
| BP\_300 | Use managed services | N |
| BP\_301 | Optimize your use of hardware-based compute accelerators | N |
| Sustainability | How do you select Regions for your workload? | BP\_302 | Choose Region based on both business requirements and sustainability goals | Y |
| Sustainability | How do you take advantage of software and architecture patterns to support your sustainability goals? | BP\_303 | Optimize software and architecture for asynchronous and scheduled jobs | N |
| BP\_304 | Remove or refactor workload components with low or no use | N |
| BP\_305 | Optimize areas of code that consume the most time or resources | N |
| BP\_306 | Optimize impact on devices and equipment | N |
| BP\_307 | Use software patterns and architectures that best support data access and storage patterns | N |
| Sustainability | How do you align cloud resources to your demand? | BP\_308 | Scale workload infrastructure dynamically | N |
| BP\_309 | Align SLAs with sustainability goals | N |
| BP\_310 | Stop the creation and maintenance of unused assets | N |
| BP\_311 | Optimize geographic placement of workloads based on their networking requirements | N |
| BP\_312 | Optimize team member resources for activities performed | N |
| BP\_313 | Implement buffering or throttling to flatten the demand curve | N |

# High Risk Items (Filtered View)

|  |  |  |  |
| --- | --- | --- | --- |
| **Pillar Name** | **Question** | **BP #** | **Choice (Best Practice)** |
| Cost Optimization | How do you implement cloud financial management? | BP\_4 | Establish ownership of cost optimization |
| Cost Optimization | How do you decommission resources? | BP\_14 | Decommission resources automatically |
| BP\_16 | Implement a decommissioning process |
| Cost Optimization | How do you monitor your cost and usage? | BP\_30 | Allocate costs based on workload metrics |
| BP\_32 | Identify cost attribution categories |
| BP\_33 | Establish organization metrics |
| BP\_34 | Configure detailed information sources |
| BP\_35 | Add organization information to cost and usage |
| Operational Excellence | How do you evolve operations? | BP\_69 | Implement feedback loops |
| BP\_71 | Perform operations metrics reviews |
| Operational Excellence | How do you implement observability in your workload? | BP\_81 | Implement user experience telemetry |
| BP\_82 | Implement dependency telemetry |
| BP\_83 | Implement distributed tracing |
| BP\_84 | Identify key performance indicators |
| Operational Excellence | How do you know that you are ready to support a workload? | BP\_113 | Ensure personnel capability |
| BP\_114 | Use playbooks to investigate issues |
| BP\_115 | Use runbooks to perform procedures |
| Performance Efficiency | How do you select and use compute resources in your workload? | BP\_122 | Use optimized hardware-based compute accelerators |
| BP\_124 | Scale your compute resources dynamically |
| Performance Efficiency | How do you select and configure networking resources in your workload? | BP\_135 | Evaluate available networking features |
| BP\_136 | Use load balancing to distribute traffic across multiple resources |
| Reliability | How do you design your workload to adapt to changes in demand? | BP\_153 | Use automation when obtaining or scaling resources |
| BP\_154 | Load test your workload |
| BP\_155 | Obtain resources upon detection that more resources are needed for a workload |
| BP\_156 | Obtain resources upon detection of impairment to a workload |
| Reliability | How do you use fault isolation to protect your workload? | BP\_161 | Deploy the workload to multiple locations |
| BP\_162 | Select the appropriate locations for your multi-location deployment |
| BP\_163 | Automate recovery for components constrained to a single location |
| BP\_164 | Use bulkhead architectures to limit scope of impact |
| Reliability | How do you manage service quotas and constraints? | BP\_165 | Automate quota management |
| BP\_166 | Accommodate fixed service quotas and constraints through architecture |
| BP\_167 | Aware of service quotas and constraints |
| BP\_168 | Manage service quotas across accounts and Regions |
| BP\_170 | Ensure that a sufficient gap exists between the current quotas and the maximum usage to accommodate failover |
| Reliability | How do you design interactions in a distributed system to mitigate or withstand failures? | BP\_171 | Set client timeouts |
| BP\_172 | Implement emergency levers |
| BP\_173 | Fail fast and limit queues |
| BP\_174 | Implement graceful degradation to transform applicable hard dependencies into soft dependencies |
| BP\_175 | Control and limit retry calls |
| BP\_176 | Make services stateless where possible |
| BP\_177 | Throttle requests |
| Reliability | How do you monitor workload resources? | BP\_179 | Monitor end-to-end tracing of requests through your system |
| BP\_181 | Define and calculate metrics (Aggregation) |
| BP\_183 | Conduct reviews regularly |
| Reliability | How do you test reliability? | BP\_202 | Test resiliency using chaos engineering |
| BP\_204 | Use playbooks to investigate failures |
| Security | How do you incorporate and validate the security properties of applications throughout the design, development, and deployment lifecycle? | BP\_220 | Automate testing throughout the development and release lifecycle |
| BP\_223 | Deploy software programmatically |
| BP\_224 | Manual code reviews |
| BP\_225 | Perform regular penetration testing |
| BP\_227 | Train for application security |
| Security | How do you classify your data? | BP\_228 | Automate identification and classification |
| Security | How do you classify your data? | BP\_230 | Identify the data within your workload |
| Security | How do you classify your data? | BP\_231 | Define data lifecycle management |

# Medium Risk Items (Filtered View)

|  |  |  |  |
| --- | --- | --- | --- |
| **Pillar Name** | **Question** | **BP #** | **Choice (Best Practice)** |
| Cost Optimization | How do you evaluate cost when you select services? | BP\_42 | Perform cost analysis for different usage over time |
| Cost Optimization | How do you meet cost targets when you select resource type, size and number? | BP\_49 | Select resource type, size, and number automatically based on metrics |
| Operational Excellence | How do you reduce defects, ease remediation, and improve flow into production? | BP\_52 | Implement practices to improve code quality |
| BP\_57 | Share design standards |
| Operational Excellence | How do you understand the health of your operations? | BP\_85 | Communicate status and trends to ensure visibility into operation |
| BP\_87 | Review operations metrics and prioritize improvement |
| Operational Excellence | How does your organizational culture support your business outcomes? | BP\_102 | Resource teams appropriately |
| Operational Excellence | How do you utilize workload observability in your organization? | BP\_116 | Analyze workload logs |
| BP\_118 | Analyze workload traces |
| BP\_120 | Create dashboards |
| Performance Efficiency | How do you select the appropriate cloud resources and architecture patterns for your workload? | BP\_143 | Use benchmarking to drive architectural decisions |
| Reliability | How do you plan for disaster recovery (DR)? | BP\_185 | Automate recovery |
| BP\_186 | Manage configuration drift at the DR site or Region |
| Reliability | How do you implement change? | BP\_210 | Deploy using immutable infrastructure |
| BP\_212 | Integrate resiliency testing as part of your deployment |
| Reliability | How do you design your workload to withstand component failures? | BP\_213 | Automate healing on all layers |
| BP\_214 | Rely on the data plane and not the control plane during recovery |
| BP\_215 | Fail over to healthy resources |
| BP\_218 | Architect your product to meet availability targets and uptime service level agreements (SLAs) |
| BP\_219 | Use static stability to prevent bimodal behavior |
| Security | How do you detect and investigate security events? | BP\_235 | Automate response to events |
| Security | How do you anticipate, respond to, and recover from incidents? | BP\_246 | Pre-deploy tools |
| Security | How do you anticipate, respond to, and recover from incidents? | BP\_247 | Pre-provision access |
| Security | How do you anticipate, respond to, and recover from incidents? | BP\_248 | Prepare forensic capabilities |

## Remediation

#### Overview

In this section we start categorizing and prioritising risk item remediations. Remediation activities are assigned an effort classification, allowing us to end up with three types of solution profiles:

* **Quick Wins** – A grouping of best-practice remediation items considered to be low hanging fruit, and easily addressable with Engineering effort allocation.
* **Projects** – Bespoke projects of varying sizes to accommodate more complex remediation items
* **CCL Products and Services** – Solutions that have been developed by CCL which directly and collectively addresses specific sets of best practice remediation items. These products and services are mapped to the impacted HRIs and MRIs.

#### Remediation Breakdown

###### Quick Wins

The following table contains risk items which are bundled together to form a DevOps and Cloud Engineering effort estimate.

|  |  |  |
| --- | --- | --- |
| **BP #** | **Best Practice Remediation** | **Risk** |
| BP\_4 | Establish ownership of cost optimization | High |
| BP\_14 | Decommission resources automatically | High |
| BP\_16 | Implement a decommissioning process | High |
| BP\_30 | Allocate costs based on workload metrics | High |
| BP\_32 | Identify cost attribution categories | High |
| BP\_33 | Establish organization metrics | High |
| BP\_34 | Configure detailed information sources | High |
| BP\_35 | Add organization information to cost and usage | High |
| BP\_69 | Implement feedback loops | High |
| BP\_71 | Perform operations metrics reviews | High |
| BP\_81 | Implement user experience telemetry | High |
| BP\_82 | Implement dependency telemetry | High |
| BP\_83 | Implement distributed tracing | High |
| BP\_84 | Identify key performance indicators | High |
| BP\_113 | Ensure personnel capability | High |
| BP\_114 | Use playbooks to investigate issues | High |
| BP\_115 | Use runbooks to perform procedures | High |

1. **Establish ownership of cost optimization (BP\_4):** Assign a dedicated team or individual responsible for monitoring and managing cloud costs. This involves setting up processes, governance, and reporting mechanisms. Define roles and responsibilities clearly.
2. **Decommission resources automatically (BP\_14) & Implement a decommissioning process (BP\_16):** Develop automated scripts or use cloud management tools to identify unused or underutilized resources and decommission them. Understand the customer environment and identify safe criteria for decommissioning.
3. **Allocate costs based on workload metrics (BP\_30):** Implement tagging and cost allocation reports to distribute costs accurately across different departments or projects. This requires a clear understanding of the customer organizational structure and workload distribution.
4. **Identify cost attribution categories (BP\_32), Establish organization metrics (BP\_33), Configure detailed information sources (BP\_34), Add organization information to cost and usage (BP\_35):** These practices involve enhancing the granularity and relevance of cost reporting. Customer collaboration is required to define cost categories, set up the necessary data collection, and configure reports accordingly.
5. **Implement feedback loops (BP\_69):** Set up mechanisms to collect and analyse operational data to improve processes continuously. Identify key metrics, establish feedback channels, and integrate insights into operational practices.
6. **Implement user experience telemetry, dependency telemetry, and distributed tracing (BP\_81, BP\_82, BP\_83):** Deploy monitoring tools and services to gain insights into application performance and dependencies. This will require collaboration with the customer's development and operations teams to integrate these tools into their systems and workflows.
7. **Identify key performance indicators (BP\_84):** Define and measure KPIs that align with the customer’s business objectives and operational goals. This involves analysing current operations, setting targets, and implementing measurement tools.
8. **Ensure personnel capability (BP\_113), Use playbooks to investigate issues, and Use runbooks to perform procedures (BP\_114, BP\_115):** Develop training programs and documentation to enhance the team's skills and efficiency. In collaboration with the customer, Identify knowledge gaps, develop training materials, and create procedural documentation.

**Combined Estimate:**

The time required to implement these quick wins can vary based on the customer's current infrastructure, the complexity of their environment, and the level of collaboration. However, a rough estimate for implementing all these quick wins could be:

* Initial setup and planning: 1-2 weeks
* Implementation and deployment (parallelizable tasks): 2-4 weeks
* Monitoring, optimization, and handover: 1-2 weeks

**Total: 4-8 weeks** for complete implementation across all identified quick wins. This estimate assumes that tasks can be executed concurrently and that there is active participation and collaboration from the customer. Note: This is just a rough estimate – details to be finalised, should a SOW be requested.

###### Remediation Projects

The following projects are identified as potential solutions for further consideration. In most cases, CCL will be able to undertake any of these projects from a Professional Services perspective.

* + - 1. Secure Data Management and Compliance

This project aims to enhance data security and compliance with regulatory requirements. It will focus on classifying, encrypting, and securely managing data both at rest and in transit within the AWS environment.

**Scope**

Classification and encryption of sensitive data, implementation of data lifecycle policies, and ensuring data integrity and confidentiality.

**Deliverables**

* Data classification framework and implementation.
* Encryption mechanisms for data at rest and in transit.
* Access control policies and mechanisms for data security.
* Compliance reporting and audit trail mechanisms.

The following table contains risk items which are bundled together to form a Project and a high-level effort estimate.

|  |  |  |
| --- | --- | --- |
| **BP #** | **Best Practice Remediation** | **Risk** |
| BP\_228 | Automate identification and classification | High |
| BP\_231 | Define data lifecycle management | High |
| BP\_271 | Enforce encryption at rest | High |
| BP\_276 | Enforce encryption in transit | High |

**High-level** **Effort estimate:** 6-8 weeks

* + - 1. Resilience and Disaster Recovery Planning

This project is focused on enhancing the resilience and disaster recovery capabilities of the AWS environment. It aims to ensure business continuity by implementing robust failover mechanisms, backup and restore procedures, and multi-region deployment strategies.

**Scope**

Implementation of disaster recovery strategies, backup and restore procedures, and cross-region redundancy.

**Deliverables**

* Disaster recovery plan and procedures.
* Automated backup and restore mechanisms.
* Multi-region deployment and failover strategies.
* Testing and validation of disaster recovery procedures.

The following table contains risk items which are bundled together to form a Project and a high-level effort estimate.

|  |  |  |
| --- | --- | --- |
| **BP #** | **Best Practice Remediation** | **Risk** |
| BP\_155 | Obtain resources upon detection of need | High |
| BP\_156 | Obtain resources upon detection of impairment | High |
| BP\_185 | Automate recovery | High |
| BP\_210 | Deploy using immutable infrastructure | High |

**High-level** **Effort estimate:** 8-10 weeks

* + - 1. Identity and Access Management Optimisation

This project aims to improve security posture by enhancing identity and access management (IAM) practices. It will focus on implementing least privilege access, managing permissions, and automating credential rotation.

**Scope**

Review and optimization of IAM policies, implementation of least privilege access, and automation of credential management.

**Deliverables**

* Updated IAM policies and roles.
* Least privilege access implementation report.
* Automated mechanisms for credential rotation and management.
* Training and documentation for IAM best practices.

The following table contains risk items which are bundled together to form a Project and a high-level effort estimate.

|  |  |  |
| --- | --- | --- |
| **BP #** | **Best Practice Remediation** | **Risk** |
| BP\_236 | Audit and rotate credentials periodically | High |
| BP\_259 | Grant least privilege access | High |
| BP\_260 | Manage access based on lifecycle | High |
| BP\_239 | Rely on a centralized identity provider | High |

**High-level** **Effort estimate:** 4-6 weeks

###### CCL Products and Services

No Additional CCL Products or Services have been identified beyond the scope of the Quick Wins and Projects detailed above.

## Conclusion

The customer workload review reports a **moderate** score with relation to the AWS Well-Architected Framework, with a clear remediation focus required on the following pillar(s):

* Reliability

With clear remediation mapping pathways established to Quick Wins, Projects, and CCL Products and Services, we are confident that this workload can experience great improvements along the 6 Pillars and an overall reduction in risk.

It is worth noting that this WAFR has been performed on non-critical workload as part of AWS MAP. Considering the nature of the workload, and the current priorities of AgResearch, there is no immediate action/remediation required. The migration project can continue, and future refinement of WAFRs based on successful workload migrations will ultimately inform AgResearch’s roadmap. Should this WAFR be regarded in isolation, the below can be noted for future conversations:

**Immediate Next Steps:**

1. **Review and Prioritize**: Collaborate with your teams to review the findings and prioritize remediation efforts based on impact and feasibility.
2. **Plan and Allocate Resources**: Based on priorities, plan the allocation of resources to address the Quick Wins immediately and schedule Project work.
3. **Engage with CCL**: For specialized support, consider engaging with CCL for professional services tailored to your specific needs and challenges.

**Roadmap for WAFR Remediation / Implementation**:

* **0-3 Months**: Focus on Quick Wins to gain immediate improvements and build momentum. Begin detailed planning and start the implementation of the first set of Projects.
* **3-6 Months**: Continue with the implementation of Projects, based on the prioritized list. Start measuring improvements and refining practices based on feedback.
* **6-12 Months**: Evaluate the progress made on the Projects. Begin integrating CCL Products and Services where applicable. Review and adjust the roadmap based on the results achieved and lessons learned.

As part of the CCL WAFR offering, a fast-tracked Statement of Work can be generated upon customer request, ensuring a seamless transition from planning to action.

# WAFR Risk Breakdown Yeehaw