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:**

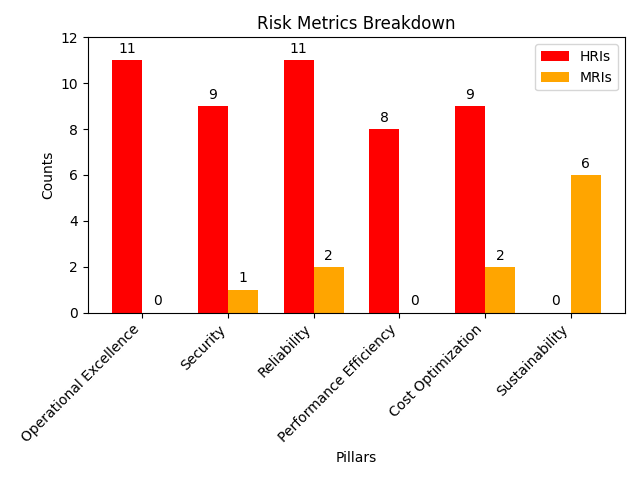
* Operational Excellence
* Security
* Reliability
* Performance Efficiency
* Cost Optimisation
* Sustainability

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 | 11 | 0 | 0 |
| Security | 0 | 9 | 1 | 0 |
| Reliability | 0 | 11 | 2 | 0 |
| Performance Efficiency | 0 | 8 | 0 | 0 |
| Cost Optimization | 0 | 9 | 2 | 0 |
| Sustainability | 0 | 0 | 6 | 0 |



# High Risk Items

|  |  |  |
| --- | --- | --- |
| **Pillar Name** | **Question Title** | **Best Practice Choice** |
| Operational Excellence | OPS 1. How do you determine what your priorities are? | Evaluate governance requirements |
| Evaluate compliance requirements |
| Evaluate threat landscape |
| 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 |
| Team members are enabled and encouraged to maintain and grow their skill sets |
| Resource teams appropriately |
| Diverse opinions are encouraged and sought within and across teams |
| 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 6. How do you mitigate deployment risks? | 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 |
| Operational Excellence | OPS 7. How do you know that you are ready to support a workload? | Ensure consistent review of operational readiness |
| Use runbooks to perform procedures |
| Use playbooks to investigate issues |
| Make informed decisions to deploy systems and changes |
| Enable support plans for production workloads |
| 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 |
| Define escalation paths |
| Define a customer communication plan for outages |
| Communicate status through dashboards |
| Automate responses to events |
| Security | SEC 1. How do you securely operate your workload? | Identify and validate control objectives |
| Keep up-to-date with security threats |
| Keep up-to-date with security recommendations |
| Identify threats and prioritize mitigations using a threat model |
| Automate testing and validation of security controls in pipelines |
| Evaluate and implement new security services and features regularly |
| Security | SEC 4. How do you detect and investigate Security events? | Configure service and application logging |
| Analyze logs, findings, and metrics centrally |
| Automate response to events |
| Implement actionable security events |
| Security | SEC 5. How do you protect your network resources? | Control traffic at all layers |
| Automate network protection |
| Implement inspection and protection |
| Security | SEC 6. How do you protect your compute resources? | Perform vulnerability management |
| Reduce attack surface |
| Implement managed services |
| Automate compute protection |
| Enable people to perform actions at a distance |
| Validate software integrity |
| Security | SEC 7. How do you classify your data? | Identify the data within your workload |
| Define data protection controls |
| Automate identification and classification |
| Define data lifecycle management |
| Security | SEC 8. How do you protect your data at rest? | Enforce encryption at rest |
| Automate data at rest protection |
| Enforce access control |
| Use mechanisms to keep people away from data |
| Security | SEC 9. How do you protect your data in transit? | Implement secure key and certificate  management |
| Enforce encryption in transit |
| Automate detection of unintended data  access |
| Authenticate network communications |
| Security | SEC 10. How do you anticipate, respond to, and recover from incidents? | Develop incident management plans |
| Automate containment capability |
| Pre-provision access |
| Pre-deploy tools |
| Run game days |
| Reliability | REL 1. How do you manage service quotas and constraints? | 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 |
| Reliability | REL 3. How do you design your workload service architecture? | Choose how to segment your workload |
| Build services focused on specific business domains and functionality |
| 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 |
| Reliability | REL 6. How do you monitor workload resources? | 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) |
| Analytics |
| Conduct reviews regularly |
| Monitor end-to-end tracing of requests through your system |
| Reliability | REL 8. How do you implement change? | 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 |
| Reliability | REL 9. How do you back up data? | Identify and back up all data that needs to be backed up, or reproduce the data from sources |
| 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? | Deploy the workload to multiple locations |
| Use bulkhead architectures to limit scope of impact |
| Automate recovery for components constrained to a single location |
| Performance Efficiency | PERF 1. How do you select the best performing architecture? | Define a process for architectural choices |
| Factor cost requirements into decisions |
| Use policies or reference architectures |
| Benchmark existing workloads |
| Load test your workload |
| Performance Efficiency | PERF 2. How do you select your compute solution? | 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 |
| Continually evaluate compute needs based on metrics |
| Performance Efficiency | PERF 3. How do you select your storage solution? | Understand storage characteristics and requirements |
| Evaluate available configuration options |
| Make decisions based on access patterns and metrics |
| Performance Efficiency | PERF 4. How do you select your database solution? | 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 |
| Performance Efficiency | PERF 5. How do you configure your networking solution? | Understand how networking impacts performance |
| Evaluate available networking features |
| Choose appropriately sized dedicated connectivity or VPN for hybrid workloads |
| Choose network protocols to improve performance |
| Optimize network configuration based on metrics |
| Performance Efficiency | PERF 6. How do you evolve your workload to take advantage of new releases? | Stay up-to-date on new resources and services |
| Define a process to improve workload performance |
| Evolve workload performance over time |
| Performance Efficiency | PERF 7. How do you monitor your resources to ensure they are performing? | 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 |
| Performance Efficiency | PERF 8. How do you use tradeoffs to improve Performance Efficiency? | Learn about design patterns and services |
| Measure the impact of performance improvements |
| Use various performance-related strategies |
| Cost Optimisation | COST 2. How do you govern usage? | Develop policies based on your organization requirements |
| Implement cost controls |
| Cost Optimisation | COST 3. How do you monitor usage and cost? | 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 |
| Cost Optimisation | COST 4. How do you decommission resources? | Track resources over their life time |
| Enforce data retention policies |
| Decommission resources automatically |
| Cost Optimisation | COST 5. How do you evaluate cost when you select services? | 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 |
| 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 pricing models for all components of this workload |
| Perform pricing model analysis at the master account level |
| 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 |
| Cost Optimisation | COST 10. How do you evaluate new services? | Develop a workload review process |
| Review and analyze this workload regularly |

# Medium Risk Items

|  |  |  |
| --- | --- | --- |
| **Pillar Name** | **Question Title** | **Best Practice Choice** |
| Security | SEC 3. How do you manage permissions for people and machines? | Establish emergency access process |
| Reduce permissions continuously |
| Share resources securely within your organization |
| Share resources securely with a third party |
| Manage access based on life cycle |
| Analyze public and cross-account access |
| Reliability | REL 2. How do you plan your network topology? | 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 |
| Reliability | REL 7. How do you design your workload to adapt to changes in demand? | Load test your workload |
| Cost Optimisation | COST 1. How do you implement cloud financial management? | Monitor cost proactively |
| Quantify business value from cost optimization |
| Report and notify on cost optimization |
| Sustainability | SUS 1. How do you select Regions for your workload? | Choose Region based on both business requirements and sustainability goals |
| Sustainability | SUS 2. How do you align cloud resources to your demand? | Scale workload infrastructure dynamically |
| Optimize geographic placement of workloads based on their networking requirements |
| Align SLAs with sustainability goals |
| Stop the creation and maintenance of unused assets |
| Optimize team member resources for activities performed |
| Implement buffering or throttling to flatten the demand curve |
| 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? | Implement a data classification policy |
| Use policies to manage the lifecycle of your datasets |
| Use elasticity and automation to expand block storage or file system |
| Remove unneeded or redundant data |
| Use shared file systems or storage to access common data |
| Minimize data movement across networks |
| Back up data only when difficult to recreate |
| Use technologies that support data access and storage patterns |
| Sustainability | SUS 5. How do you select and use cloud hardware and services in your architecture to support your Sustainability goals? | Use the minimum amount of hardware to meet your needs |
| Use instance types with the least impact |
| Use managed services |
| Optimize your use of hardware-based compute accelerators |
| Sustainability | SUS 6. How do your organizational processes support your Sustainability goals? | Adopt methods that can rapidly introduce sustainability improvements |
| Keep your workload up-to-date |
| Increase utilization of build environments |
| Use managed device farms for testing |

## Remediation Plan

### Quick Wins

|  |  |  |
| --- | --- | --- |
| **#** | **Question** | **Best Practice** |
| 1 | OPS 1. How do you determine what your priorities are? | Evaluate governance requirements |
| 2 | OPS 1. How do you determine what your priorities are? | Evaluate compliance requirements |
| 3 | OPS 1. How do you determine what your priorities are? | Evaluate threat landscape |
| 4 | SEC 4. How do you detect and investigate security events? | Configure service and application logging |
| 5 | SEC 4. How do you detect and investigate security events? | Analyze logs, findings, and metrics centrally |
| 6 | SEC 4. How do you detect and investigate security events? | Automate response to events |
| 7 | SEC 4. How do you detect and investigate security events? | Implement actionable security events |
| 8 | COST 3. How do you monitor usage and cost? | Configure detailed information sources |
| 9 | COST 3. How do you monitor usage and cost? | Identify cost attribution categories |
| 10 | COST 3. How do you monitor usage and cost? | Establish organization metrics |

#### Evaluate governance requirements

##### Description

Assess governance requirements and align priorities to meet those requirements.

##### Remediation

Form a working group to review current governance policies and requirements. Identify any gaps where existing priorities may not satisfy requirements. Develop a prioritization framework that ensures governance requirements are met while still enabling the business. Communicate new priorities across teams.

##### Additional Considerations

Consider regulatory compliance requirements and involve key stakeholders when setting priorities.

##### Effort Estimate

2 week effort: 1 week to collect requirements, 1 week to align priorities

##### Resourcing and Skills

Governance team, key business stakeholders

##### Domain Impact

Governance, Legal/Compliance

#### Evaluate compliance requirements

##### Description

This quick win focuses on evaluating compliance requirements to help determine priorities.

##### Remediation

A detailed analysis should be conducted of all relevant compliance requirements and standards. These should be mapped to current operations to determine gaps, priorities, and next steps. Both internal policies and external regulations should be considered.

##### Additional Considerations

When evaluating compliance requirements, be sure to take a risk-based approach focused on the highest priority obligations. Continually revisit this analysis as new requirements emerge.

##### Effort Estimate

2 week quick-win effort: - 1 week to compile all compliance requirements - 1 week to map requirements to current operations and document gaps and priorities

##### Resourcing and Skills

Security and compliance expert to understand requirements; Operations leads to analyze current practices

##### Domain Impact

This would primarily impact security, compliance, and operations.

#### Evaluate threat landscape

##### Description

Assess the current threat landscape and identify the top risks and threats to prioritize for remediation

##### Remediation

Perform an evaluation of the existing controls and safeguards to identify gaps in security defenses. Research threat intelligence from industry reports and news to determine high risk threats that apply to the organization's environment. Create a prioritized list of threats and vulnerabilities to address based on potential business impact.

##### Additional Considerations

When evaluating threats, take organizational factors into account such as compliance requirements, industry standards, geographic location, and other business drivers that may influence risk tolerance.

##### Effort Estimate

2 weeks for initial assessment and prioritization; ongoing threat monitoring

##### Resourcing and Skills

Security analyst and architect to perform assessment; access to threat intelligence feeds

##### Domain Impact

Security

#### Configure service and application logging

##### Description

Enable AWS CloudTrail logging across all accounts to capture API calls and log them to S3. Configure VPC Flow Logs on all VPCs. Enable CloudWatch logging for EC2, Lambda, and other services.

##### Remediation

1. Enable CloudTrail in all accounts and log to a centralized S3 bucket. Use CloudTrail Lake for analytics.   
2. For all VPCs, enable VPC Flow Logs to capture network traffic logs. Send to S3 and analyze with services like Athena.   
3. For EC2 instances, Lambda functions, and other supported services, enable CloudWatch Logs with appropriate log retention policies. Send logs to S3 for long term archival.

##### Additional Considerations

Logs should be encrypted at rest using KMS. Redact sensitive data before storing logs. Send critical logs to security monitoring tools like GuardDuty.

##### Effort Estimate

CloudTrail and VPC Flow logs can be enabled with Terraform/CloudFormation scripts across accounts. Per-service logging may require additional effort to tune log retention and storage.

##### Resourcing and Skills

Cloud platform engineer, security engineer, DevOps engineer to implement logging and monitoring architecture.

##### Domain Impact

Primarily benefits security domain with increased visibility into API calls, network traffic, and application logs for incident investigation.

#### Analyze logs, findings, and metrics centrally

##### Description

Centralize log, findings, and metrics analysis to improve security event detection and investigation.

##### Remediation

Implement a central security analytics solution like AWS Security Hub to aggregate findings from services like AWS GuardDuty. Build custom metrics and dashboards in Amazon CloudWatch to detect anomalies. Use Amazon Athena to query logs in Amazon S3.

##### Additional Considerations

Consider the volume of logs and findings generated to size analytics services appropriately. Roll out changes incrementally to measure impact.

##### Effort Estimate

Quick win estimated as 2 weeks to set up initial AWS Security Hub integration and custom CloudWatch metrics

##### Resourcing and Skills

Security analyst, CloudWatch expert, Security Hub administrator

##### Domain Impact

Security

#### Automate response to events

##### Description

Implement automated response and remediation workflows for detected security events using AWS services

##### Remediation

Leverage Amazon EventBridge to set up automated event-driven security workflows. Define rules to match security events from services like AWS Security Hub, GuardDuty, Macie etc. and trigger target responses such as AWS Lambda functions to run automated remediation playbooks. Consider using services like AWS Step Functions to model more complex workflows.

##### Additional Considerations

Ensure adequate testing of automated response workflows before deploying to production. Adjust rule thresholds carefully to reduce false positives. Continue manual oversight and have rollback procedures in place.

##### Effort Estimate

This is a low effort quick win that can be implemented within 2-4 weeks.

##### Resourcing and Skills

Security architect, DevOps engineer familiar with infrastructure-as-code

##### Domain Impact

Security

#### Implement actionable security events

##### Description

Implement capabilities to detect and investigate security events in the environment

##### Remediation

Enable CloudTrail logging across all accounts and integrate the logs with a SIEM solution like Amazon Macie. Configure Macie to detect unusual API calls and user activities and trigger alerts. Build an incident response playbook to investigate the alerts.

##### Additional Considerations

Consider least privilege access for cross account roles used by Macie. Tune the Macie alerts to reduce false positives.

##### Effort Estimate

2 weeks for initial CloudTrail and Macie setup. Ongoing tuning of alerts.

##### Resourcing and Skills

Cloud security engineer to setup and configure CloudTrail, Macie, and SIEM integration. Security analysts to investigate alerts.

##### Domain Impact

Security

#### Configure detailed information sources

##### Description

Enable detailed monitoring in AWS Cost Explorer to track usage and cost at granular levels.

##### Remediation

1. In the AWS Billing Console, navigate to Cost Explorer. 2. In the left pane, choose Cost & Usage Reports. 3. Choose Create report. 4. Enter a Report name and select the required Report time granularity. 5. In the Include resource IDs section, select Yes. 6. In the Report data section, select Include and choose Resource IDs from the drop-down list. 7. Choose Next. 8. On the Deliver report page, configure the S3 bucket to receive the reports. 9. Choose Next then Review and Complete to create the report.

##### Additional Considerations

Detailed AWS Cost and Usage reports can help attribute spends to specific services, resources, tags, and other dimensions. Schedule automatic generation and archiving of these reports for better insights.

##### Effort Estimate

1. Enable detailed cost and usage reporting in Cost Explorer - 0.5 days. 2. Configure automatic generation and archiving - 0.5 days.

##### Resourcing and Skills

User with permissions to configure cost and usage reporting in AWS Billing Console.

##### Domain Impact

Finance

#### Identify cost attribution categories

##### Description

Implement tagging and cost allocation reporting to attribute costs to departments, projects, applications etc.

##### Remediation

1. Design a taxonomy of tags aligned to the business, considering attributes like department, project, application etc.   
2. Develop policies and procedures to ensure tags are applied properly in account provisioning and resource deployment.   
3. Configure detailed cost allocation reports in AWS Cost Explorer based on tags.   
4. Socialize reports with business leaders to facilitate cost ownership.

##### Additional Considerations

Tagging discipline is critical to enable precise cost visibility. Reports should be easy to understand for non-technical business owners.

##### Effort Estimate

Quick win requiring 1 week for tag design and 3 weeks for implementation.

##### Resourcing and Skills

Cloud Economist, Account Admin, Infrastructure Owner

##### Domain Impact

Finance

#### Establish organization metrics

##### Description

Implement metrics and alarms for tracking overall AWS costs against targets

##### Remediation

1. Identify key cost metrics at organization and account level based on business needs, such as overall AWS spend, monthly projections vs actuals, spend by service, etc.   
2. Set up CloudWatch alarms on the key metrics versus predefined thresholds based on targets and budgets. Receive notifications when approaching or exceeding limits.  
3. Display metrics on management dashboards with drilldown to details. Review and act on alarms.

##### Additional Considerations

When implementing metrics and alarms:   
- Verify accuracy of billing and usage data   
- Clean up unused resources to avoid noise   
- Assign accountability for responding to alarms

##### Effort Estimate

Quick win, around 2 weeks effort:  
- 1 week to define metrics and alarms  
- 1 week to implement dashboards

##### Resourcing and Skills

Cloud economist, solutions architect, devops engineer

##### Domain Impact

Finance