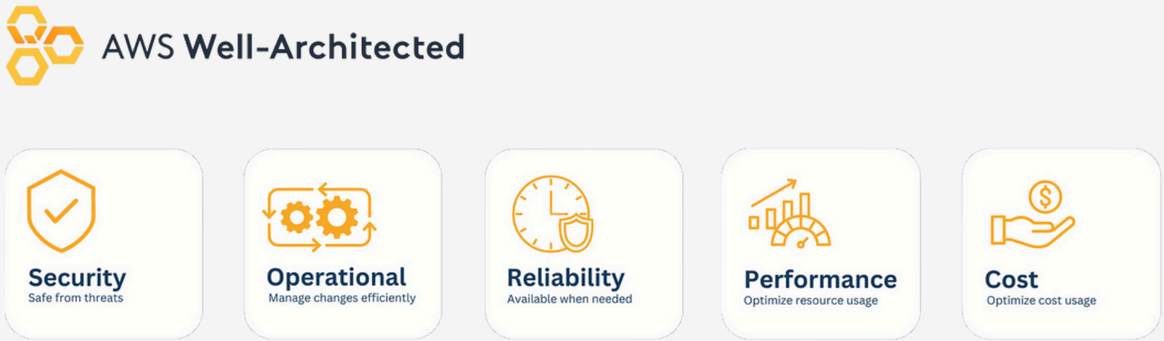
AWS Well-Architected Framework Review

January 2025

Today's **Agenda**

- AWS WAFR Overview
- Summary Findings
- Proposed Roadmap
- Open Discussion

What is the AWS Well-Architected Review?



"The Well-Architected Framework is designed to provide you with high-level guidance and best practices to help you build and maintain secure, reliable, performant, cost optimized, and operationally excellent applications in the AWS Cloud."

- AWS Well-Architected Framework Whitepaper

Well-Architected Review Goals

As Defi.App continues to scale their cloud application, the team engaged Sela to highlight the AWS best practices most relevant to their account. The goals of this review include:

Minimize system failures and operational costs

Dive deep into business and infrastructure processes

Provide best practice guidance

Delivering on the cloud computing value proposition

Pillars of the AWS Well-Architected Framework

Operational Excellence:
The ability to run and monitor systems to deliver business value and to continually improve supporting processes and procedures.

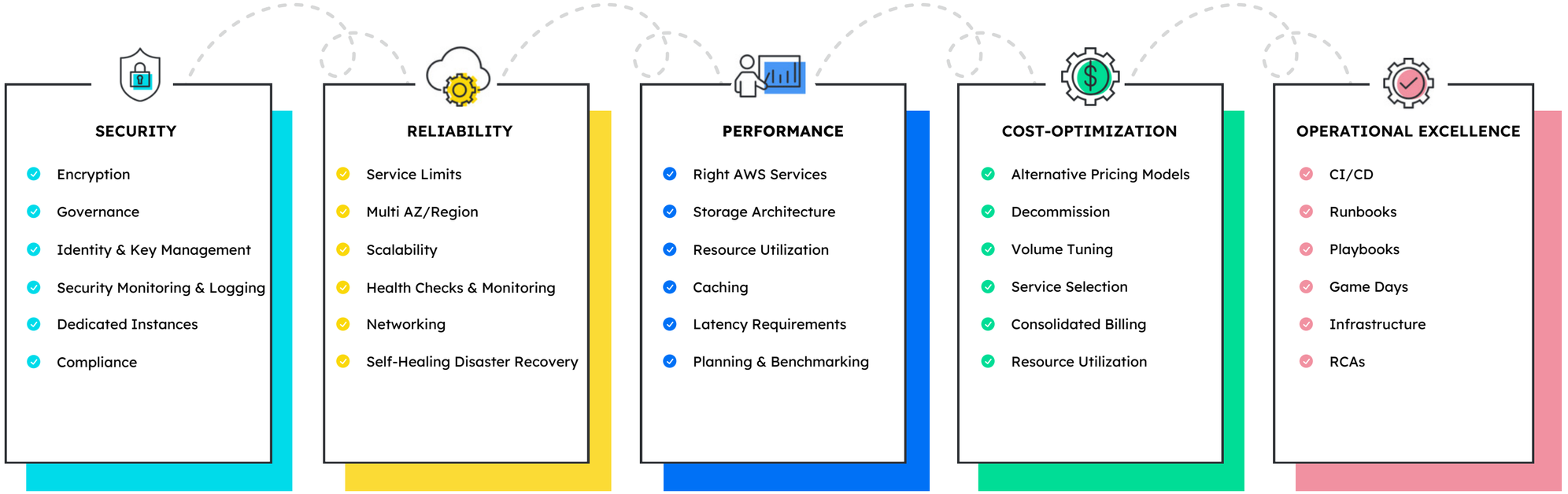
Security:
The ability to protect information, systems, and assets while delivering business value through risk assessments and mitigation strategies.

Reliability:
The ability of a system to recover from infrastructure or service failures, dynamically acquire computing resources to meet demand, and mitigate disruptions such as misconfigurations or transient network issues.

Performance Efficiency:
The ability to use computing resources efficiently to meet system requirements, and to maintain that efficiency as demand changes and technologies evolve.

Cost Optimization:
The ability to avoid or eliminate unneeded cost or suboptimal resources.

Our Approach to the AWS Well-Architected Framework



We used a standardized methodology to collaborate closely with your team, conducting a comprehensive review of your workload. This resulted in a detailed report with actionable items and tailored guidance to address key architectural pillars and resolve any architectural concerns.

Sela.

Security Findings

Sela.

Security – High Risk Issues (HRI)

Focus	Risk Assessment	Remediation
Separate dev/prod workloads into separate accounts	High	• Development resources should not share a subnet, VPC, or accounts with production resources. • Separate accounts create blast radius boundaries for automated deployments / human access
IAM improvements	High	• Remove the following IAM users: lambda-deployer, temporaryCDKuser • Replace with IAM Identity center users / oidc users. • Identity provider for AWS should be centralized directory, like Google Workspaces / O365.
Enforce encryption of data at rest	High	
Network security improvements	High	• RDS and ECS tasks have public ip address and are reachable over the internet. • Client VPN should be put in place and network interfaces should be placed in private subnets • Overlapping networks for dev / prod / staging • Naming: production VPC subnets and NAT Gateways are prefixed with staging-vpc. eg: prodVpcStack/staging-VPC/PublicSubnet2 • Security group strategy: 1 security group per component. eg: Load balancer has its own security group, defi backend service has its own security group, paymaster service has its own security group, RDS database has its own security group, Lambda has its own security group, redis has its own security group. Zero trust network rules should be applied using these security group rules rather than attaching all of them to prod service for instance.

Operational Excellence

Sela.

Operational Excellence
High Risk Issues (HRI)

Focus	Risk Assessment	Remediation

Deployment Processes	High	• Mitigate deployment risks
		  ◦ Playbooks / Change managemenet policies
		  ◦ Automate testing, integration, deployment and rollback

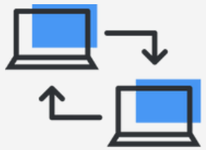
Service Runbooks, Playbooks, and Policies	High	• Manage workload and operations events
		  ◦ Runbooks / Incident Response Plans
		  ◦ Create a process for event, incident and problem management
		  ◦ Automate responses to events

Operational Excellence Medium Risk Issues (MRI)

Focus	Risk Assessment	Remediation

Operational KPIs	Medium	• Evolve operations
		  ◦ Create a process for continuous improvement
		  ◦ Perform post-incident analysis
		  ◦ Define drivers for improvement

Sela.



Reliability

Sela.

Reliability – High Risk Issues (HRI)

Focus	Risk Assessment	Remediation
Service Availability	High	• Single Node in RDS production postgres • Single redis node in production (single point of failure) ◦ Turn on availability zone rebalancing in ECS
Disaster recovery	High	• Define recovery objectives for downtime and data loss • Automate recovery • Backup data regularly and establish retention policy ◦ Currently, only RDS is backed up for 9 days

Reliability- Medium Risk Issues (MRI)

Focus	Risk Assessment	Remediation
Manage service quotas and constraints	Medium	• Accommodate fixed service quotas through architecture • Ensure that a sufficient gap exists between the current quotas and the maximum usage to accommodate failover
Workload Protection	Medium	• Deploy workloads to multiple locations – multi-zone or multi-region

Sela.

Performance Efficiency

Sela.

Performance Efficiency – Medium Risk Issues (MRI)

Focus	Risk Assessment	Remediation

Workload Efficiency	Medium	• **Establish processes to support performance efficiency in the workloads**
		  ◦ Establish key performance indicators (KPIs) to measure workload health and performance
		  ◦ Use monitoring solutions to understand the areas where performance is most critical
		  ◦ Load test the workloads
		  ◦ Define a process to improve workload performance

Workload Scaling	Medium	• Autoscaleworkloads where possible ◦ Dynamically scale your ECS services based on performance metrics.

Sela.

Cost Optimization

Sela.

Cost Optimization – High Risk Issues (HRI)

Focus	Risk Assessment	Remediation

Cloud financial management	High	• Implement cloud financial management and govern usage
		  ◦ Establish ownership of cost optimization
		  ◦ Establish cloud budgets and forecasts
		  ◦ Implement cost awareness in your organizational processes
		  ◦ Quantify business value from cost optimization
		  ◦ Report and notify on cost optimization
		  ◦ Implement goals and targets
		  ◦ Implement cost controls – tagging and allocation
		  ◦ Separate dev / prod / staging aws accounts to get better granular understanding of where money is being spent
		  ◦ Leverage reservations to optimize cost for long-running services

Right-size, fix over-provisioned resources	High	• Over-provisioned ECS services in dev, and paymaster service in prod. • Potential memory leak in backend-service as service memory steadily climbs before seemingly resetting. • No service autoscaling ECS • Database looks overprovisioned at a glance.

Cost Optimization – Medium Risk Issues (MRI)

Focus	Risk Assessment	Remediation

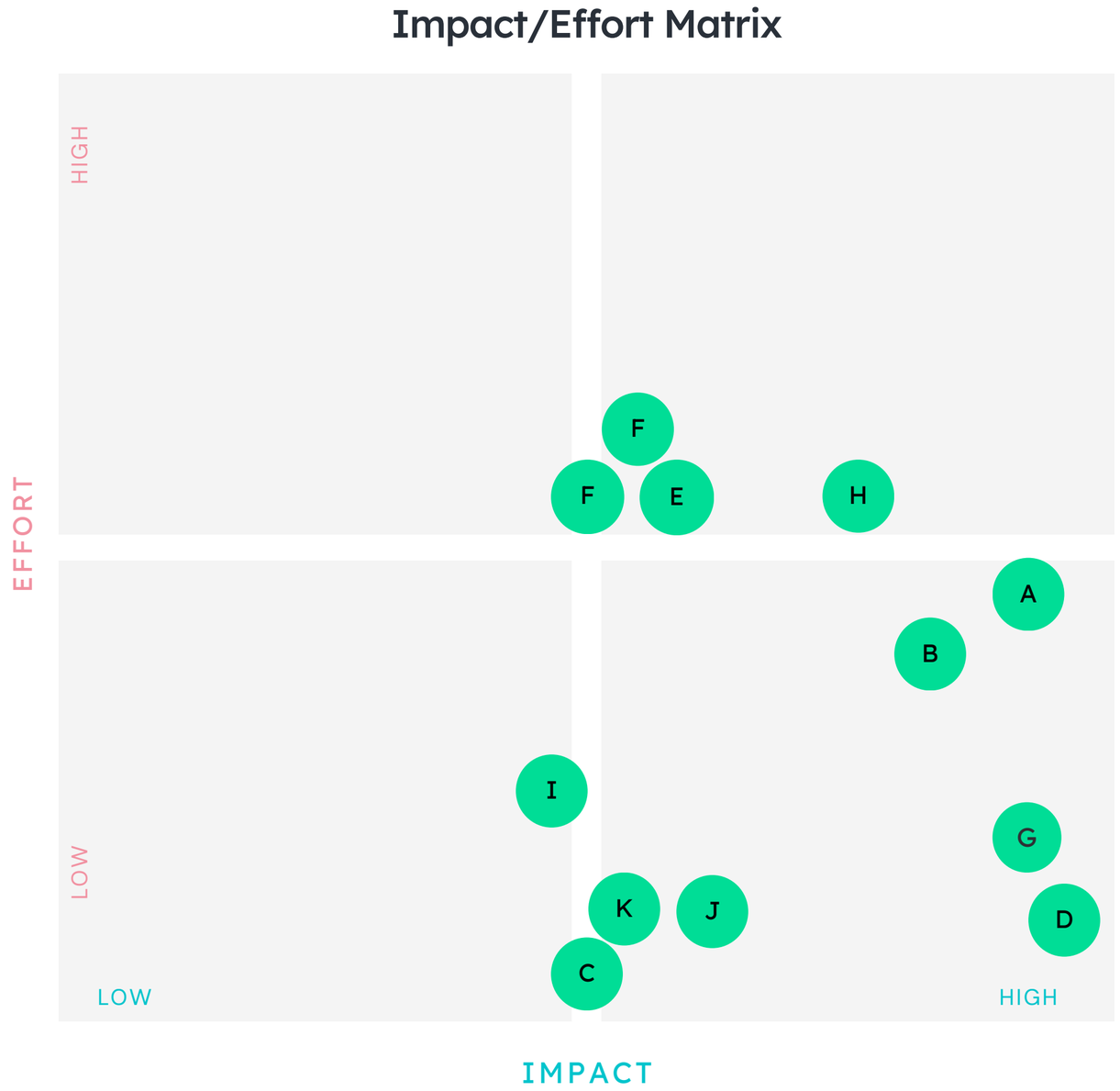
Cost Evaluation	Medium	• Evaluate cost when selecting services
		  ◦ Identify organization requirements for cost
		  ◦ Perform cost analysis for different usage over time

Resource Management	Medium	• Manage demand and resources
		  ◦ Perform ongoing analysis of the workload demands
		  ◦ Supply resources dynamically

Best Practice Improvements

Project List

Harden network security A	Separate workloads into separate accounts B
Implement IAM improvements C	Enforce encryption of data at rest D
Deployment Processes E	Service Runbooks, Playbooks, and Policies F
Service availablity G	Disaster Recovery strategy H
Implement cloud financial management and govern usage I	Enable cost alerting and analysis J
Right-size and fix over-provisioned resources K	



Customer Action Items

HRI

Months 1-3

- Isolate development from production in separate subnets or VPCs.
- Encrypt data at rest
- Deploy across multiple availability zones.
- Harden network security especially moving private endpoints to private subnets
- Separate environments into separate accounts to enhance fault isolation / security boundary
- Set budgets and use reservations for cost optimization.
- Implement disaster recovery plan and perform table-top exercises

MRI

Months 3-6

- Create a security response plan with incident exercises and scans.
- Automate event management and responses.
- Architect for service quotas with capacity for failover.
- Use KPIs, monitoring, and load tests for performance efficiency.
- Adjust resources dynamically to manage costs and demand.

Reevaluate

Months 6-9

- Revisit areas identified as no improvements to maintain status and reduce risk
- Revisit runbooks and security policies to ensure they still apply to organization
- Identify new opportunities for cost optimization

Discussion