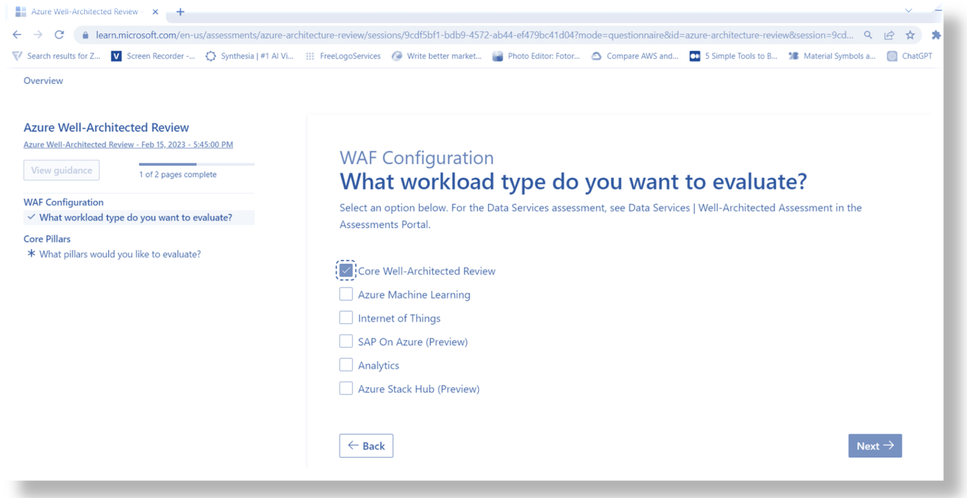
Effective Well Architected Review

facts, experiential learning, insights & contextualization



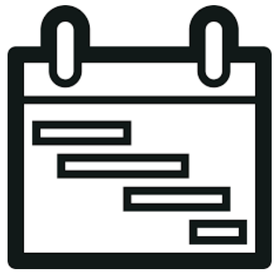
CODINGRANGE

CSP Guidance + Tool + Expertise + Impact Analysis, Business Objective

CODINCITY
CODING THE FUTURE

Approach and Methodology

- Industry recognized, professionally qualified resources
- 15 – 20 yrs experienced architects with proven record
- Experience with delivering Well Architected Reviews
- Hand-On with IaaS, PaaS and Serverless technologies
- AWS Certified Well Architected Partner*



Detailed Planning

Curated AI Applied Knowledge Base

Tools

Collaboration

Review / Feedback

$12000 pa savings opportunities identified for start-up product company in the USA

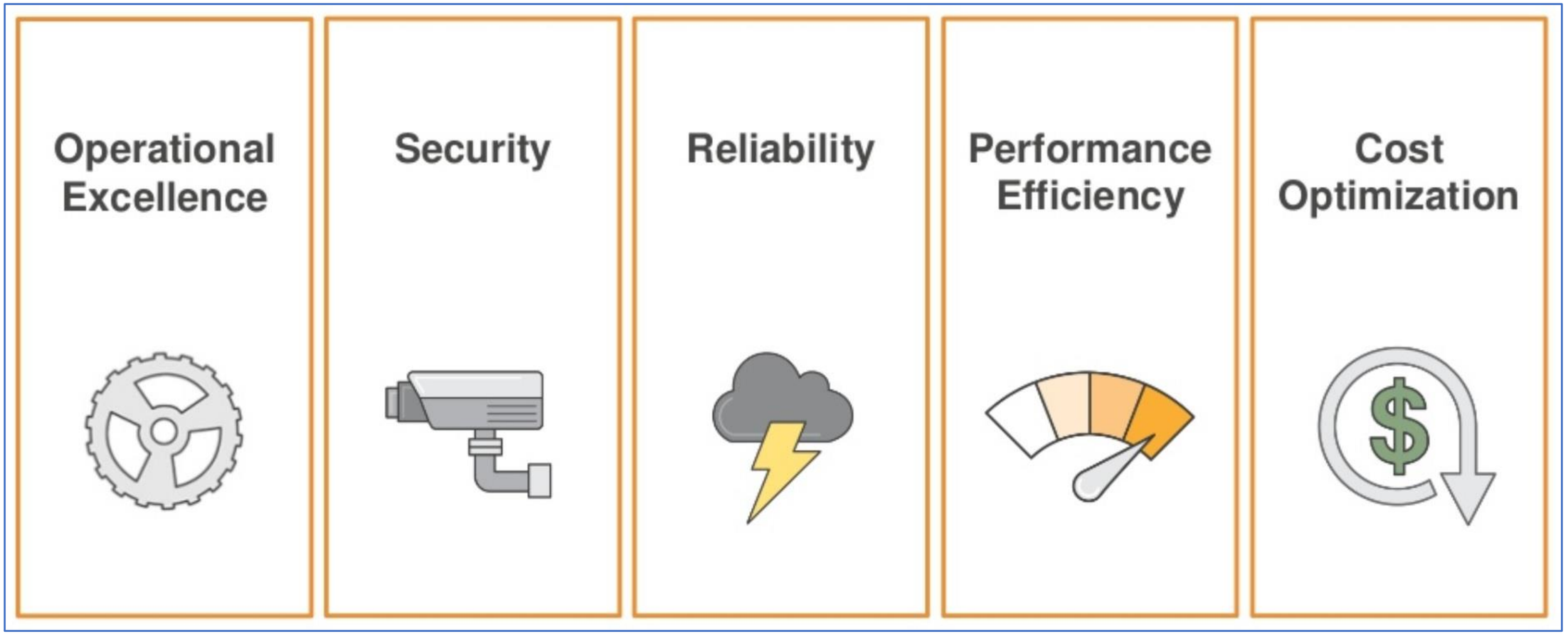
From un-known to confident security posture journey for a FinTech loan origination application in 6 weeks

Frequent application downtime to 24x7 availability for a Site Safety Management company in the USA

CODINCITY
CODING THE FUTURE

Well Architected Review Framework

Multi-dimensional review against industry best practices



CODINCITY
CODING THE FUTURE

From Cloud Naïve to Cloud Native

Elevate Cloud Experience, Save Cost, Harness Cloud Potential

Microsoft
Solutions Partner

Infrastructure
Azure

Microsoft
Solutions Partner

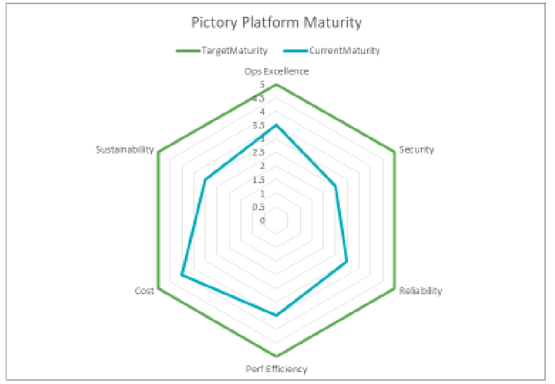
Digital & App Innovation
Azure

Benefit from our superior skillset, innovative solution, tools and services

CODINCITY
CODING THE FUTURE

Sample Report

Summary – Well Architected Review for <customer> Cloud Platform



- Average platform maturity that can be improved with a few quick remediations
- 14 high risk and 14 medium risks identified, across parameters of assessment
- Overall, 37 recommendations for improving platform maturity are provided along with priority.
- Some of the audit questions are called out as out of scope given the application size, and current business priorities
- A couple of third-party tools are recommended to be evaluated vis-à-vis native services and/or manual processes
- Due to the smaller environment size and limited dependencies, most of the remediations actions can be performed with little impact on application availability

- Findings, potential impact and remediation actions with costs
- Prioritization of actions based on business needs, application road map, constraints, cost-benefits
- Cost Savings opportunities
- Third-party , fit-for-purpose solutions evaluation

Assessment – Security : key findings, remediation & cost-implications

S#	Priority	Finding	Implication	Remediation	Costs/ month	Status	Comments
1	1	Root Account MFA not enabled	1. Gives all access, including change of support plan, account closure 2. Against best practices	1. Enable MFA for root user 2. Delete any access keys	NA		1. Account Owner/ designated person to enabled MFA using software token like Google Authenticator on phone ; Codincity will guide, if necessary https://docs.aws.amazon.com/accounts/latest/reference/root-user-tasks.html
2	1	Unnamed/generic users	1. Difficult to trace activities 2. Against best practices	1. Create groups with specific access for a role 2. Create individual users	NA		1. Example user accounts – devops_admin_1
3	1	Delete inactive users, Access keys not rotated for long time	1. Data loss , unauthorized activity in the account including launching costly resources	1. Delete inactive users 2. Rotate access keys 3. Assign password policy	NA		1. Review users, groups – create additional groups, if needed ; update policies with least privileges required for job . 2. Rotate credentials 3. Assign password policy
4	1	CloudTrail is not enabled for management actions	1. Inability identify malicious actions performed by user(s)	1. Enable Cloud Trail for management events	$5 to $10		1. Given the limited number of AWS Users, the number events is expected to small 2. Improve traceability for future compliance
5	1	GuardDuty not enabled	1. Real-time threat detection is not possible (e.g. brut force attack, suspicious credentials/activities)	1. Enable GuardDuty for Ohio region	$20 to $40		1. GuardDuty detects suspicious activities and looks through VPC flowlogs, DNS logs and audit trail
6	1	SGs have 0-65535 ports open to internet	1. Increased attack surface	1. Restrict security group inbound port to required ones like 80and 443 2. Delete unused SG	NA		1. 27 Security groups are found ; Only a SG named default is used for NLB/ALB 2. No credentials hence unable to find details – to request additional access from Shailendra
7	2	Default VPCs present in 17 regions, application workload only in one region	1. It's possible to launch resources in regions outside Mumbai, even with limited access	1. Delete Default VPC	NA		1. Default VPCs in unused regions is a vulnerability

Summary – Overall Cost (savings)/addition

SNo	Cost Component	Increase or Decrease	Estimated Annual (Savings) Additional cost	Comments
1	Savings Plan for better coverage	Decrease	(3600)	1. At a minimum $300 per month, based on current utilization statistics
2	S3 lifecycle / intelligent tiering	Decrease	(3600)	1. Approx 300 per month savings assuming 50:30:20 tiering
3	Delete unused resources - ELBs, EIP	Decrease	(240)	1. Rough estimate of $20 per month
3	Optimization of ECS Task definition and usage	Decrease	(6000)	1. Using lower sized containers, evaluating current usage trend from cloudwatch – estimated savings of $500 per month
4	AWS WAF implementation	Increase	1200	1. With 5 ruleset for most common attacks prevention
6	GuardDuty implementation	Increase	600	1. Enabling guardDuty on a Ohio region
7	CloudTrail enhancement to include management actions	Increase	600	1. Add on spend of 50 per month to include additional events
8	Enable config rules / conformance packs	Increase	600	
		TOTAL	(4440) – w/o ECS task optimization (10440) – with ECS task optimization	

CODINCITY
CODING THE FUTURE