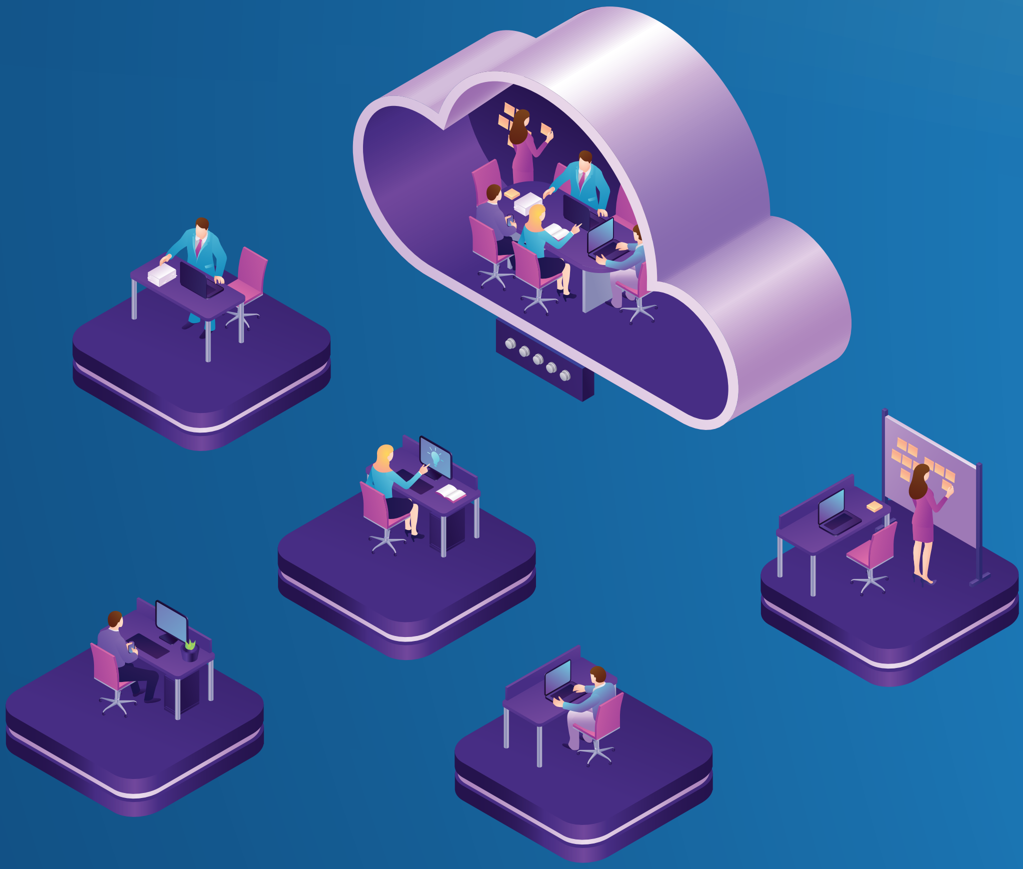
LTIMindtree

BUILDING A CLOUD ADOPTION STRATEGY

A PRACTICAL GUIDE TO POTENTIAL SUCCESS.



Contents

1. **Preface** 3
2. **Chapter 1 -** Is cloud the right choice? 4
3. **Chapter 2 -** Cloud adoption strategy & its importance 7
4. **Chapter 3 -** Understanding the lifecycle of cloud adoption 12
5. **Chapter 4 -** Get started with comprehensive cloud assessment 17
6. **Chapter 5 -** Cloud migration framework that works 30
7. **Chapter 6 -** Cloud Center Of Excellence: The rising trend among enterprises 35
8. **Chapter 7 -** The 4 DevOps: DevOps, FinOps, SecOps, CloudOps 38
9. **Chapter 8 -** The rise of cloud Governance 41
10. **Chapter 9 -** A deep dive on cloud security 44
11. **Chapter 10 -** Importance of continuous modernization on cloud 48
12. **Chapter 11 -** The cloud is much more than just hosting: Data, AI, ML, IoT 50
13. **Conclusion** 53

PREFACE

There is no denying the ubiquity of cloud computing, which has now become a part of a CIO's daily lexicon. Within the last decade, led by born-in-the-cloud startups like Netflix, Spotify have brought cloud from the fringes to the centre of any enterprise IT strategy. What the cloud has also done is bring about great democratisation, where both an enterprise or a startup has access to the same cutting edge technology at scale. The shattering of these barriers has given birth to the adage - **beginning of the end of software as we know it**. Further validated by the rapid adoption of cloud across its various modules led by SaaS, followed by IaaS growing the fastest along with PaaS integration, all contributing to a market worth $266 billion in 2020 as per Gartner; a 10X growth in the last decade.

However, as is with things of great impact and further compounded with the vagaries of each organisation, the question arises 'What is the right way ... to adopt cloud for my organisation?'. Take the example of a successful diet+exercise plan, it is very individualistic, needs very clearly defined goals and most importantly is to be followed diligently. The cloud is very similar, in order to have high impact, there is a need for a well-constructed plan to make it's adoption a design rather than an (unintended) consequence.

In the last 10 years, I have been a part of several large cloud adoption journeys ranging from large global enterprises to single app startups, and in most cases resulting in significant business impact. I recall one journey, where a digital insurance company grew almost by 1000% Y-o-Y for 3 consecutive years, largely enabled by their cloud adoption. Another with a large life sciences software company, who moved 4000+ applications and 15,000+ servers to the cloud, this modernisation exercise greatly enhanced their eventual $1B valuations. I would also like to remark that there have also been failures too, though unfortunate, these have also greatly contributed to my learnings.

This document is a compilation of my experiences and is not intended to define a singular path to success, but rather an illustrated assortment of strategies that have worked. I hope by the end of this document, you the reader would have a greater practical understanding of how one could drive success through the adoption of some best practices.

CHAPTER 1

Is Cloud the Right Choice?

Some existential questions before we jump in, and I bring up the diet+exercise analogy again - take the vegan 'fad' (yes there is a body of evidence to substantiate that, but that's a discussion for another day), just because some celebrity garners huge social validation, doesn't mean that you could turn vegan without analyzing relevance to you. This decision should not be an outward-in decision, but rather an inward-out out. You need to analyze your current eating habits, allergies, calorie needs, physical activity, and lifestyle to conclude if turning vegan would be good for you.

The choices around the adoption of cloud follow a similar disposition. Any under-analysed approach, sometimes triggered by peer replication or analysts posturing, could potentially result in failure. Forbes predicts that 80% of all enterprise (and mission-critical) workloads will move to the cloud by 2025. Yes, an overwhelming statistic and the cloud does bring definite advantages, but forcing a system that is not designed or optimised for the cloud does more disservice in the long term.

Hence critically analyze the benefits of cloud on your business, collect the relevant data points, simulate the business behaviour, and then arrive at an empirical conclusion. If you are still unsure after, try an incremental modernization approach (which I cover in detail later) as a gauged exercise.

So to get started, what are the questions that you can ask yourself to know if the cloud is the right choice for you?

Cost Driver	• Am I running my on-premise IT infrastructure efficiently? Will I save more by moving to the cloud? • Are my overhead costs in managing on-premise IT infrastructure more than my peers who are on the cloud? • Will my CFO prefer moving to an OPEX model instead of the current CAPEX model? • Does moving from traditional enterprise software to cloud-based open-source platforms help me free from the stronghold of large enterprise technology companies?
Technology Driver	• If I am covered on the cost, do I see an advantage of modernization by moving to the cloud?

	• Can the leverage cloud services in AI, ML, IoT, Data to add value to my business?
People Driver	• Will I continue to get good talent to manage my non-cloud IT setup while the ecosystem appears to be adopting cloud faster? • Will I be able to retain good talent if I enable them with learning new technologies like a cloud?
Operations Driver	• Will adopting cloud help me automate the IT processes like DevOps, incident management, remediation, backups, DR, etc? • Can cloud reduce the IT infrastructure provisioning time which will allow my technology team to move faster?
Innovation Driver	• Can I use some of the cutting-edge cloud service offerings to drive innovation in my organization?

If you find yourself answering more questions in the positive, you know which direction you need to be going. However, before we go forward let's bust some myths, if we may:

5 Myths of Cloud Transformation

Moving to the cloud saves cost

Note always true, while moving might reduce cost but as a result of proper/institutionalised cloud management. The core objectives to move should be to achieve operational excellence, drive competitive advantage like scalability, agility and seamless access to future-proof technology.

Cloud is just an extension of my existing (on-prem) environment

It is important to understand and appreciate the cloud as a completely different environment altogether which requires both technical and cultural re-invention. A simplistic transposing to the cloud will meet with challenges and diminish the extractable value.

Cloud can manage itself

In continuation of the above, while the cloud does offer a lot of automation and platform-based services, that, however, does not completely absolve supervision. Critical enablers of success.

still require human design/intervention, bringing areas like governance (covered later in the document) to the forefront.

Cloud should replace everything

An all-in approach should be based on clear organizational priorities and the back of reasonable expectations. If it ain't broke don't fix it, perform various analyses, and try to figure out which is more in line with your organizational needs, replace only if necessary.

The cloud is fail-proof

Even with all the advantages cloud brings it still isn't fail-proof and a granular understanding of the T&C by the provider is critical. This along with robust governance protocols and it's implementations are imperative to mitigate risks.

CHAPTER 2

Cloud Adoption Strategy and its Importance

The definition of a cloud strategy is important because an incorrect strategy can potentially set you back by several years, leading to having to play catch up vis-a-vis moving ahead. There are 4 important considerations to deliberate that could help arrive at an effective cloud strategy.

1. Business Case

Do not start building your cloud strategy without building your business case first! Many cloud adoption journeys end up with cost and governance issues due to a lack of a unified and clear business case. I have witnessed several cases where the CIOs push on cloud adoption without a business, and this has proven fatal.

A business case importantly helps you map to larger organization goals with clearly articulated benefits. These business cases are either be built individually at the application level and cumulatively, giving you both a segmented and overall view.

A robust business case should ideally address the below-mentioned parameters across the functions

Parameters	Business Decision	IT Decision	Rating
Results in Cost Savings	Y		8
Improves Application Availability & Scalability	Y	Y	10
Improves Infrastructure Reliability		Y	8
Enables Agile Development & Faster GTM		Y	8
Leverages New Cloud Technologies		Y	7
Enhances Regulations & Compliance	Y	Y	6
Improvement in Disaster Recovery & BCP process		Y	10
Improves Application Security		Y	10

Aids in Modernization of Applications		Y	6
Easier License Management		Y	5
Reduces Operational Overhead		Y	7
Improves Application Performance	Y		10
Planned for Surge in Future Growth	Y		5

A score of 50+ would make for an ideal candidate for adoption and would provide tangible results from a successful adoption.

2. Decision Framework

With the multitude of ever-increasing choices, it is important to consider these core parameters. A suggested framework like below would lay the contours of your cloud strategy.

What is the mix you would like to have?	• All-in Cloud - 100% exit from the on-premise systems • A hybrid setup with distribution between on-prem and cloud
What type of cloud best suits my organization?	• Private Cloud • Public Cloud • SaaS-based Platforms • Any combination of the above
What is the ideal combination for on cloud?	• Single Cloud • Multi-Cloud • Hybrid Cloud
Which public cloud providers will I choose?	• AWS ...

What will be my distribution of applications among the three hosting models?	● IaaS ● PaaS ● SaaS
Build vs Buy Decisions	● Buy a SaaS-based platform if it best suits the requirements ● Build a cloud-native application on public cloud
What will be my de-facto technology stack on the cloud?	● Containers ● Microservices ● Server-less ● Automated DevOps

This decision framework will help you shape up your base cloud strategy and not all of these answers will be obvious, without readily available data. A proven exercise like Migration Readiness Assessment will help you arrive at answers for most of the above questions. This could be a primer for a more comprehensive business case for each application in the overall ecosystem.

3. Importance of Data First Thinking

More often than not the core of cloud migration gets obfuscated in the applications vs Servers discussion. However, the smarter approach would be to address the core component of the migration i.e., data. Consider a scenario where you are migrating 100 applications to the cloud. Without a centralized data design plan during your migration phase, these applications will be migrated in a siloed manner. This will result in a larger footprint with disparate data systems, resulting in increased efforts to build a central data lake later to leverage the sophisticated AI/ML available on the cloud.

Hence it is very critical to define your data strategy while designing your cloud adoption strategy with better planning leading to significant time and cost savings. An example that I would like to cite here is of a large FMCG company. They during their cloud adoption strategy exercise clearly articulated the ‘data on cloud’ approach, later decided as Snowflake for data warehousing. This clarity helped develop the application migration scope with ETL components for each application built to suit the data lake plus data warehouse cloud. Saving a considerable amount of time and money and immediate realisation of the value the cloud offers.

Each organization's approach to cloud adoption varies against the various criteria stated earlier. However, all of these could be broadly clubbed under 3 common execution models.

1. The BIG BANG approach
2. The Batch Migration approach
3. Incremental Rationalization

The Big Bang Approach

The Big Bang approach is where you will decide to move all your applications, servers, data in one large migration effort, and one-time exercise. This is usually followed when there is a compelling reason and typically adopts the lift & shift approach with little or no room for modernization. These typically occur when customers have a short deadline to exit their data center. I have also come across a few scenarios where the business followed this approach when they needed to showcase significant cloud adoption to meet external demands like sale or acquisition.

Speed	High
Modernization	Low
Cost of Migration	Low
Timeline	Low

Batch Migration Approach

The second common approach followed by enterprises is the batch migration approach. CIOs resort to batch migration models in any of the below scenarios.

1. When there are budget constraints.
2. When there are allied business dependencies that need the migration to be done in batches.
3. When there are technology dependencies that require migration to be done in batches.

Dependent upon the budget and time, you can adopt a lift-shift or lift-transform-shift approach.

Speed of Migration	Moderate
Modernization	Moderate
Cost of Migration	Low
Timeline of Migration	Moderate

Incremental Rationalization (recommended)

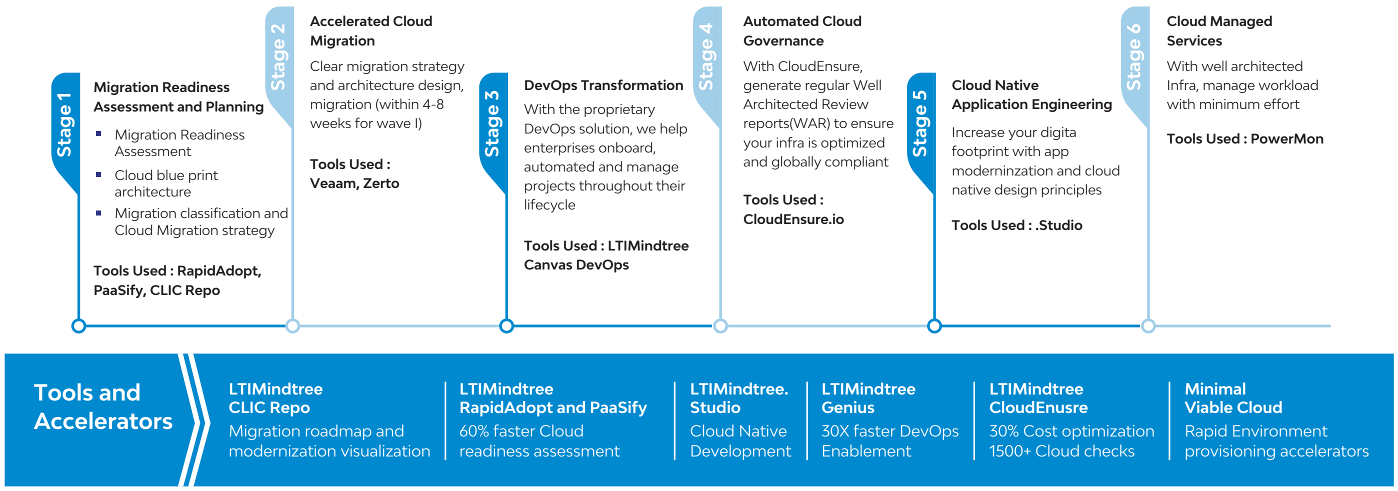
The third and the recommended model of cloud adoption is the 'incremental rationalization' model where the primary goal of cloud adoption is continuity. In this model, there are no specific schedules to do the assessment, migration, and modernization. The cloud adoption process is carried out in an agile manner keeping the whole process fluidic. Ideally, 3 different teams are involved, one for assessment, migration, and modernization each, working in parallel to have continuous adoption of cloud. I see more and more CIOs are adopting this model as this gives them the flexibility w.r.to prioritization of cloud adoption and 'manage' blockers for migration better. Consider this like your recurring deposit scheme where small continuous initiatives yield surprisingly large sum's over a period of time.

Speed of Migration	Low
Modernization	High
Cost of Migration	High
Timeline of Migration	High

CHAPTER 3

Understanding the Lifecycle of Cloud Adoption

Like the well known SDLC (Software Development Life Cycle) model, cloud adoption journey also goes through a life cycle of its own. We coined the term 'CLIC Framework' which stands for Cloud Lifecycle Framework. CLIC is now widely used by several large organizations to understand the different stages of cloud adoption and align their cloud journey progressing towards a mature cloud ecosystem.



Stage 1

Migration Readiness Assessment and Planning

- Migration Readiness Assessment
- Cloud blue print architecture
- Migration classification and Cloud Migration strategy

Tools Used : RapidAdopt, PaaSify, CLIC Repo

Stage 2

Accelerated Cloud Migration

Clear migration strategy and architecture design, migration (within 4-8 weeks for wave I)

Tools Used : Veeam, Zerto

Stage 3

DevOps Transformation

With the proprietary DevOps solution, we help enterprises onboard, automated and manage projects throughout their lifecycle

Tools Used : LTIMindtree Canvas DevOps

Stage 4

Automated Cloud Governance

With CloudEnsure, generate regular Well Architected Review reports(WAR) to ensure your infra is optimized and globally compliant

Tools Used : CloudEnsure.io

Stage 5

Cloud Native Application Engineering

Increase your digita footprint with app moderninzation and cloud native design principles

Tools Used : .Studio

Stage 6

Cloud Managed Services

With well architected Infra, manage workload with minimum effort

Tools Used : PowerMon

Tools and Accelerators

LTIMindtree CLIC Repo
Migration roadmap and modernization visualization

LTIMindtree RapidAdopt and PaaSify
60% faster Cloud readiness assessment

LTIMindtree. Studio
Cloud Native Development

LTIMindtree Genius
30X faster DevOps Enablement

LTIMindtree CloudEnusre
30% Cost optimization 1500+ Cloud checks

Minimal Viable Cloud
Rapid Environment provisioning accelerators

CLIC Framework

CLIC Framework is a proven 6-stage cloud lifecycle adoption framework which is built from the experience of helping and observing thousands of cloud adoption journeys by large enterprises. As a strong advocate of the intelligent use of tools to automate the cloud adoption process. Hence the CLIC Framework is designed to have a combination of people+process+technology at every stage of cloud adoption to ensure greater efficiency and higher success rate.

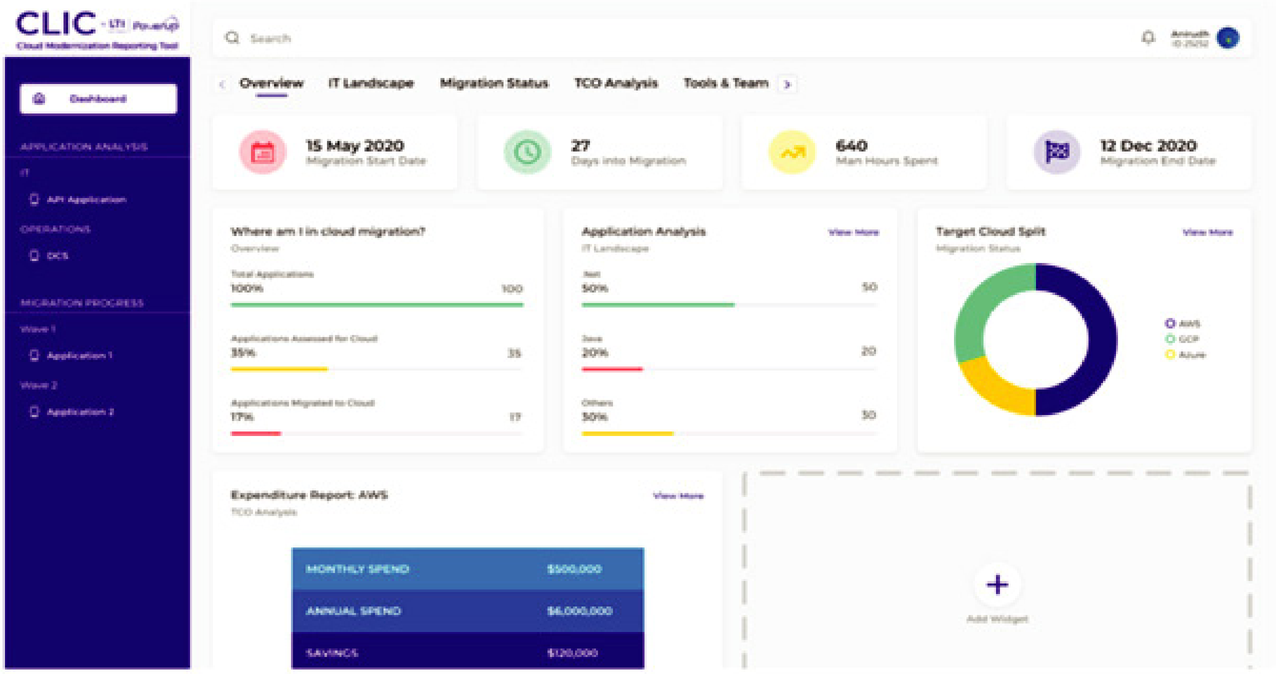
6 Stages of CLIC Framework (with our proprietary tools)

Stage	Activity	Outcomes	Toolset
Stage 1	MRAP - Migration Readiness Assessment and Planning	• Migration Readiness Assessment • TCO Analysis • Cloud Blueprint Architecture	• LTIMindtree CLIC repo • LTIMindtree RapidAdopt • LTIMindtree PaaSify • Flexera RISC Networks

		• Migration Roadmap • Migration Scope • Risks and Dependencies	
Stage 2	ACM - Accelerated Cloud Migration	• Lift-Shift • Lift-Transform-Shift • Lift-Rearchitect-Shift • Modernized Migration • Rapid Migration	• AWS Cloud Endure • LTIMindtree CLIC repo • LTIMindtree CloudEnsure
Stage 3	DATX - DevOps Automation Transformation and Modernization	• Containerization • Microservices Adoption • Serverless Architecture	• LTIMindtree CLIC repo • LTIMindtree Genius • Terraform • Kubernetes
Stage 4	ACG - Automated Cloud Governance	• Well-Architected Audit • Cloud-Native Security • Compliance Checks • FinOps and Cost Management • SecOps and Access Control	• LTIMindtree CloudEnsure • CloudHealth • CloudAbility
Stage 5	CNAE - Cloud-Native Application Engineering	• Application Modernization • Cloud-Native Development • Data Lake on Cloud • Serverless Application Development on Cloud	• LTIMindtree.Studio
Stage 6	MSP - Cloud Operations and Managed Services	• 24*7 Monitoring and Support • FinOps • DevSecOps • Incident Management	• LTIMindtree Chanak • DataDog • NewRelic

Even if you are already on the cloud, you can superimpose the CLIC Framework on your organization's adopted path and identify the gaps and areas of improvement.

To aid the cloud adoption better during the early stages of CLIC Framework, we built CLIC repo - the world's only known tool to manage the recommended Incremental Migration & Continuous Modernization.



MONTHLY SPEND	$500,000
ANNUAL SPEND	$6,000,000
SAVINGS	$120,000

Will CLIC repo move mountains?

No, not really and it's not intended to. But this is one tool that you will come to appreciate 12 months into your cloud adoption journey. Once you have your cloud strategy finalized, the execution is where most enterprises struggle.

Across my conversation with CIOs of several large enterprises, on major pain points of cloud adoption and as I quote below, a recurring theme was visibility and management during migration.

CIO of a US-based media company	"I am not able to get a complete view of migration at any given point in time. I am not able to follow the assessment and migration progress as there are multiple teams involved across multiple business units within my organization. If I can access the cloud adoption progress data, I will be able to take strategic and tactical calls which I am not able to do today."

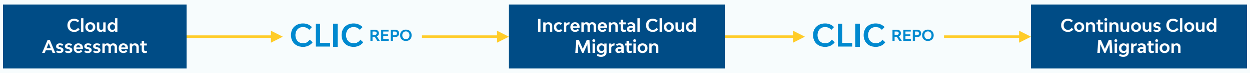
CDO of a large oil and gas corporation	"Ever since we initiated the cloud migration, my cloud costs have gone over the roof. I am spending almost twice the budgeted cloud costs and I fear that this will increase further as the project cost increases with every delay. There are no cost controls as we are still in the process of migrating to cloud. Cloud was supposed to bring down my infra spend, but the business case was proved wrong in my case due to lack of control in the migration process."

Both examples highlight one fundamental issue in their cloud migration process - transparency and control on cloud migration. These organizations have program management teams in place, but when it comes to completely transparent and highly granular info, regular BI tools don't cut the bill. There was a need for a purpose-built tool to help customers, inspiring us to build the first-ever known tool in the market to help large enterprise companies track their assessment, migration, and modernization process through a single-pane.

How can CLIC repo help you in the long run?

CLIC repo is built as a one-stop platform to help you with assessment reports, migration progress, and modernization scope for all your applications. The diagram below best illustrates how enterprises are using CLIC repo.

Across my conversation with CIOs of several large enterprises, on major pain points of cloud adoption and as I quote below, a recurring theme was visibility and management during migration.


Cloud Assessment → CLIC REPO → Incremental Cloud Migration → CLIC REPO → Continuous Cloud Migration

- Cloud assessment reports for the applications are tracked and presented through the CLIC repo tool.
- The cloud consultants can access the assessment module to conduct application stakeholder interviews and populate the business case and assessment reports for all applications considered for cloud adoption.
- The migration team picks up the cloud assessment reports which has the migration roadmap, migration plan, blueprint architecture, and other prerequisite details for cloud migration.
- The migration progress is tracked in real-time through the CLIC repo tool.

- The migration team can access the migration module to update the migration progress data.
- The modernization team takes up the applications migrated to cloud, understand the modernization scope, and executes modernization for the applications.
- The modernization team can access the modernization module to update the modernization data.

As you could see, CLIC repo turns out to be the single platform for you to access all information about your applications and acts as a central repository for all your applications under migration. The platform is built to bring in transparency across the organization on the cloud journey and forces the teams to collaborate better to handle any risks or blockers in cloud adoption.

What data can you access in the CLIC repo tool?

Assessment Track	Migration Track	Modernization Track
Business Case	Migration Roadmap	Modernization Theme
TCO Analysis	Migration Scope for an Application	Modernization Scope
Cloud Blueprint Architecture	Risks and Dependencies	Modernization Cloud Architecture
Assessment Progress	Migration Progress	Modernization Progress

CHAPTER 4

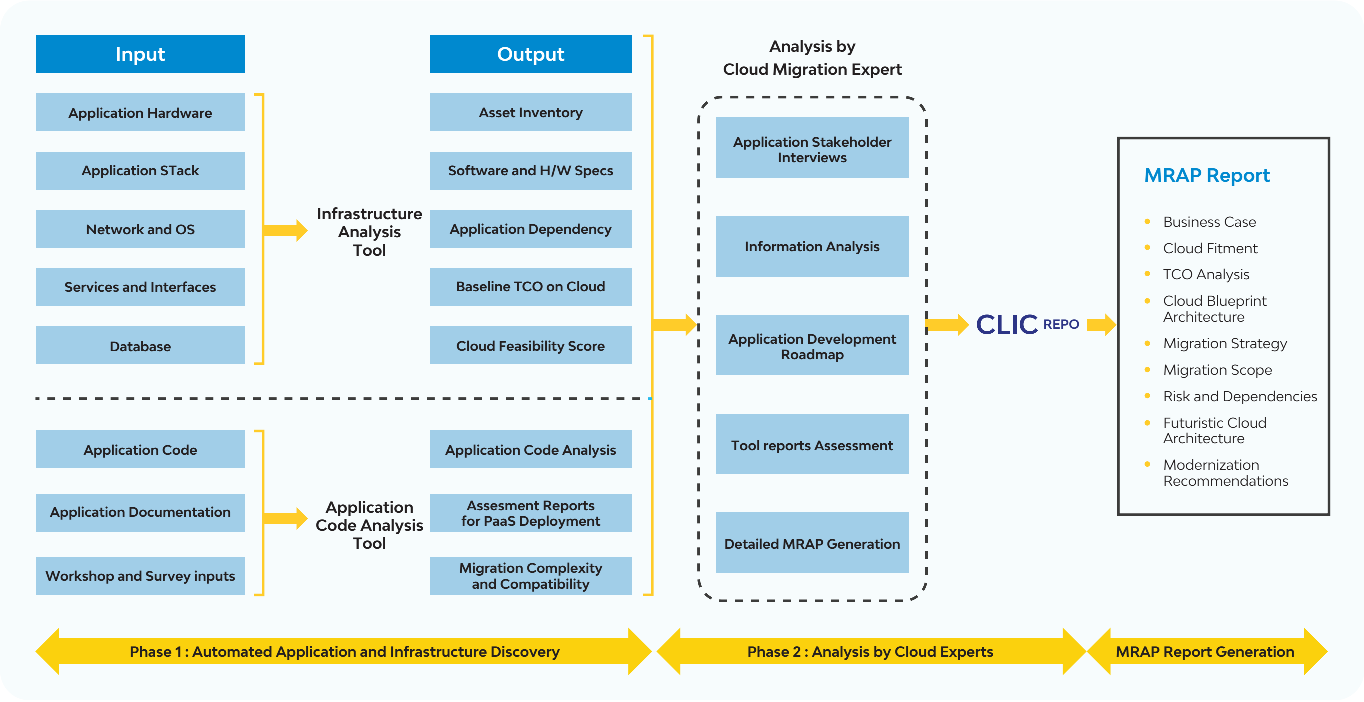
Get Started with Comprehensive Cloud Assessment

How should one go about the cloud assessment for their on-premise infrastructure? Should it be server-based or application based? From my experience, the best assessment approach that has worked for several large organizations is one where the assessment is done for applications.

The primary objective of a cloud readiness assessment is to bring in an unbiased view of the application's readiness to migrate to the cloud. If the application is better suited to run on-premise, it is advised to let it be. We define the cloud assessment process as MRAP - Migration Readiness Assessment & Planning. This is a framework inspired by the recommendations from leading cloud provider like AWS.

Migration Readiness Assessment & Planning - MRAP

MRAP is a detailed analysis of an enterprise business infrastructure and applications, led by a combination of human-machine intelligence which allows the rapid discovery of IT systems & builds a strong business case for the cloud adoption journey. The cloud assessment is done methodically to ensure that all data points of the on-premise infrastructure and applications are captured and analyzed for cloud adoption.

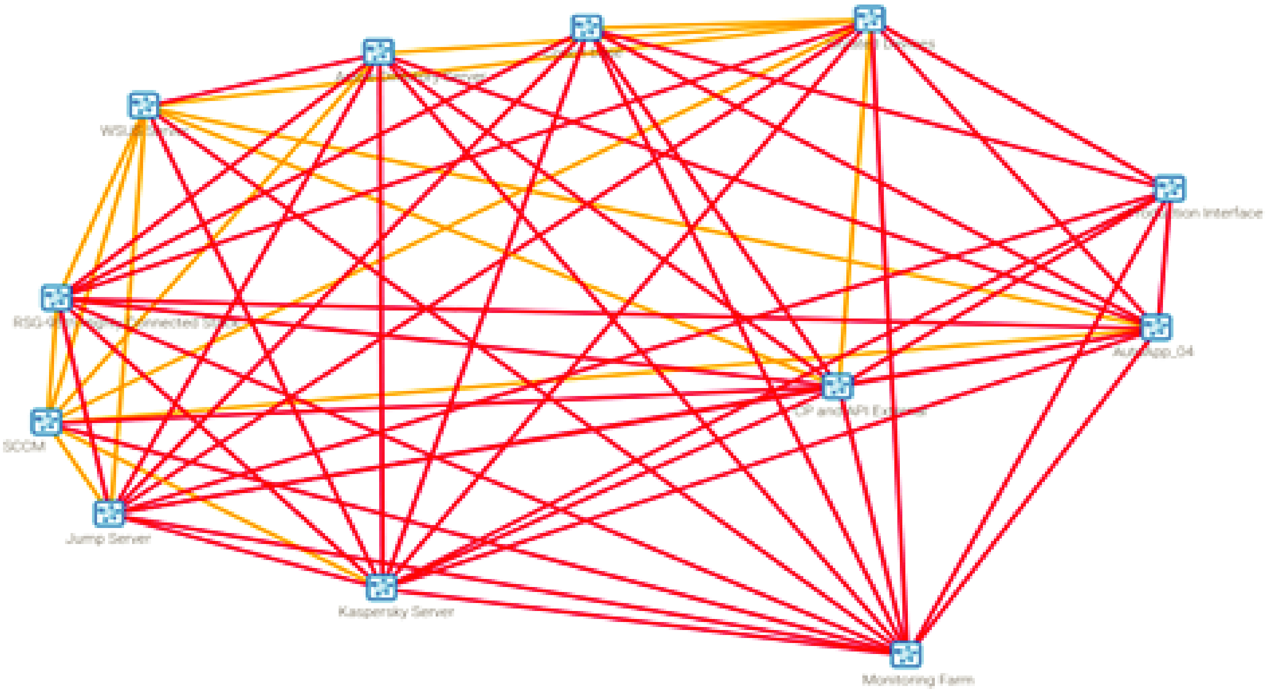

Input
Output
Analysis by Cloud Migration Expert
Application Hardware
Application STack
Network and OS
Services and Interfaces
Database
Infrastructure Analysis Tool
Asset Inventory
Software and H/W Specs
Application Dependency
Baseline TCO on Cloud
Cloud Feasibility Score
Application Code
Application Documentation
Workshop and Survey inputs
Application Code Analysis Tool
Application Code Analysis
Assesment Reports for PaaS Deployment
Migration Complexity and Compatibility
Application Stakeholder Interviews
Information Analysis
Application Development Roadmap
Tool reports Assessment
Detailed MRAP Generation
CLIC REPO
MRAP Report
Business Case
Cloud Fitment
TCO Analysis
Cloud Blueprint Architecture
Migration Strategy
Migration Scope
Risk and Dependencies
Futuristic Cloud Architecture
Modernization Recommendations
Phase 1 : Automated Application and Infrastructure Discovery
Phase 2 : Analysis by Cloud Experts
MRAP Report Generation

Phase 1: Automated Application & Infrastructure Discovery

This is the first phase of the MRAP exercise. This is highly automated in nature and the application + infrastructure discovery is carried out by intelligent assessment tools like LTIMindtree RapidAdopt, Flexera RISC Networks, AWS TSO Logic, LTIMindtree PaaSify, etc. We strongly recommend the infrastructure analysis by one of the above tools while the application codebase analysis can be considered optional. The infrastructure analysis helps the cloud migration experts get a comprehensive view of the infrastructure and associated applications. Below are the key data points collected with the help of the tool.

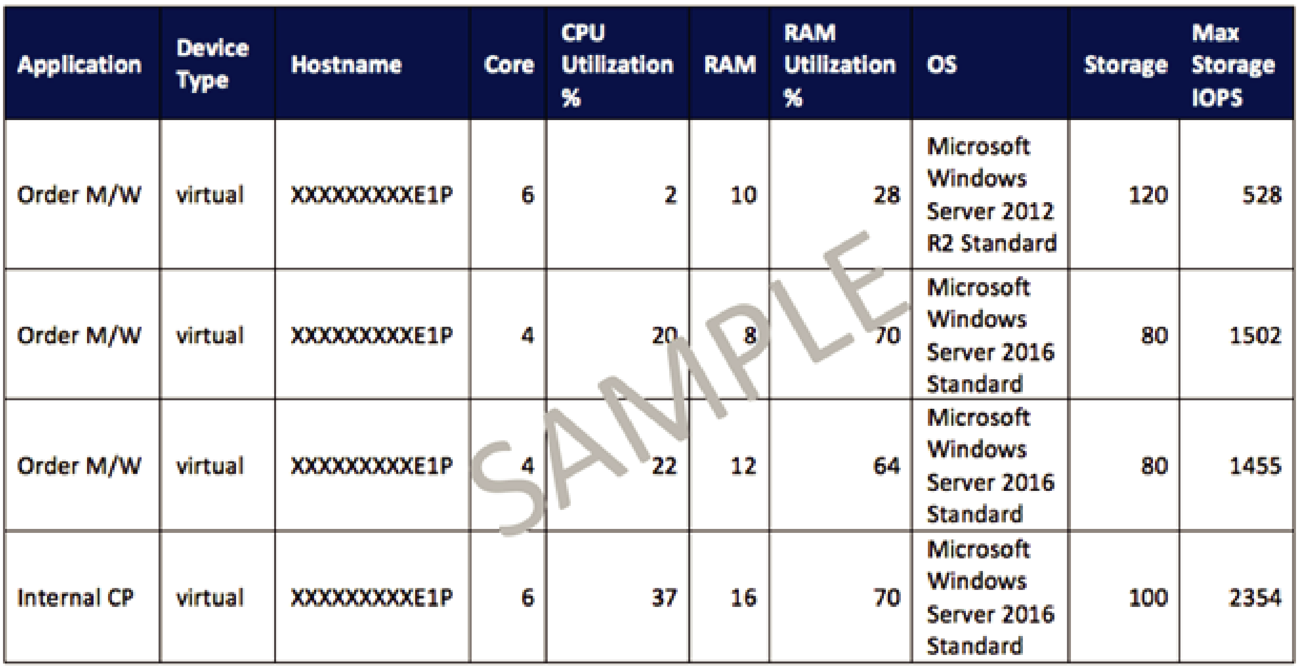
Topology Diagram of an Application

The topology of the application represents all the servers utilized by the application and their relationship. This helps us establish the connection between the applications and infrastructure inventory. This helps the team identify the servers which are not related to any application (the servers which we will consider as standalone or rogue servers) making it easier and less confusing during the analysis.



Infrastructure Utilization Details

The second key finding by the assessment tool is the comprehensive analysis of infrastructure utilization. This helps in understanding the required sizing on the cloud.



Application	Device Type	Hostname	Core	CPU Utilization %	RAM	RAM Utilization %	OS	Storage	Max Storage IOPS
Order M/W	virtual	XXXXXXXXXE1P	6	2	10	28	Microsoft Windows Server 2012 R2 Standard	120	528
Order M/W	virtual	XXXXXXXXXE1P	4	20	8	70	Microsoft Windows Server 2016 Standard	80	1502
Order M/W	virtual	XXXXXXXXXE1P	4	22	12	64	Microsoft Windows Server 2016 Standard	80	1455
Internal CP	virtual	XXXXXXXXXE1P	6	37	16	70	Microsoft Windows Server 2016 Standard	100	2354

Is the tool based application analysis mandatory?

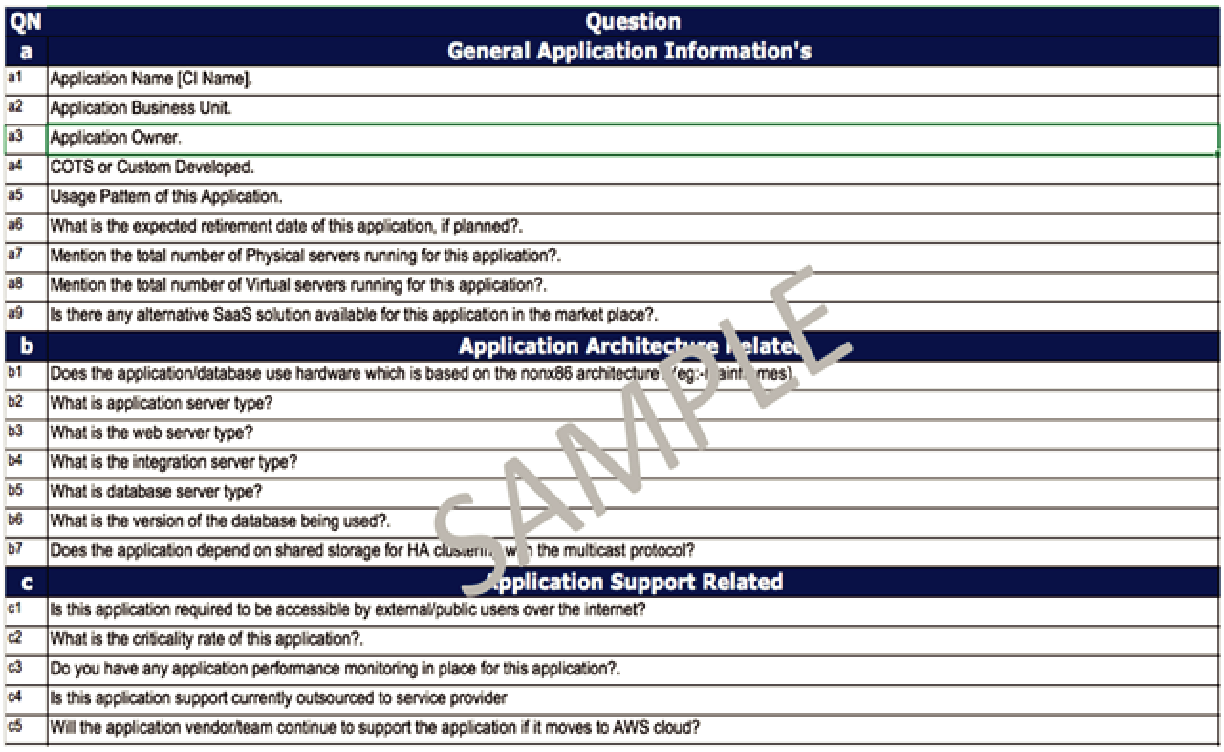
If you have the recent data on infrastructure utilization and clear mapping of the servers and hardware to applications, then the tool based assessment can be skipped. But in many cases, I see that the application and infrastructure inventory maintained by the organizations are not very accurate due to inaccuracies in the audit process, data passed between multiple teams over several years, legacy nature of applications, etc. So the tool based application analysis will help us avoid any surprises during the later stage of migration.

While these tools are very sophisticated and provide several additional intelligence including cloud resources mapping, TCO analysis, cloud fitment recommendations, I continue to find that the manual analysis conducted by the cloud migration experts in phase 2 of the MRAP exercise helps define a foolproof migration strategy. An experienced human mind can never be replaced by a tool when it comes to intuitive analysis and building a strategy.

Phase 2: Analysis by Cloud Migration Experts

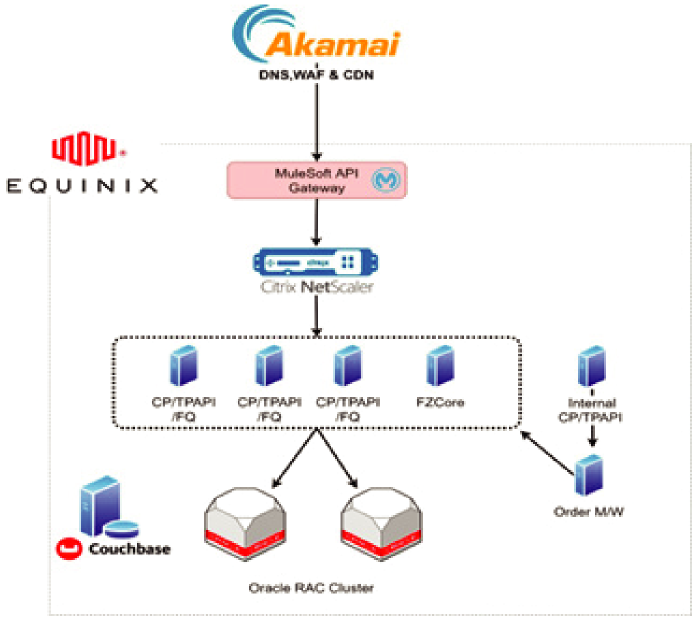
The data collected in phase 1 forms the base for the cloud migration experts to conduct a detailed study on an organization's on-premise IT landscape and derive a migration strategy that suits the organization's objectives. The migration expert will conduct stakeholder interviews, usually the application owners from business and technology teams and the infrastructure teams, to collect non-technical details of the application.

A sample stakeholder interview format is depicted below. We extensively use an automated interview form through the CLIC repo tool to conduct the data collection process. The migration experts will decide on doing a follow-up virtual interview round based on the information they see in the tool.



QN	Question
a	General Application Information's
a1	Application Name [CI Name].
a2	Application Business Unit.
a3	Application Owner.
a4	COTS or Custom Developed.
a5	Usage Pattern of this Application.
a6	What is the expected retirement date of this application, if planned?.
a7	Mention the total number of Physical servers running for this application?.
a8	Mention the total number of Virtual servers running for this application?.
a9	Is there any alternative SaaS solution available for this application in the market place?.
b	Application Architecture Related
b1	Does the application/database use hardware which is based on the nonx86 architecture (eg:-Mainframes)
b2	What is application server type?
b3	What is the web server type?
b4	What is the integration server type?
b5	What is database server type?
b6	What is the version of the database being used?.
b7	Does the application depend on shared storage for HA clustering with the multicast protocol?
c	Application Support Related
c1	Is this application required to be accessible by external/public users over the internet?
c2	What is the criticality rate of this application?.
c3	Do you have any application performance monitoring in place for this application?.
c4	Is this application support currently outsourced to service provider
c5	Will the application vendor/team continue to support the application if it moves to AWS cloud?

The migration experts will also assemble an accurate application architecture based on the analysis results of the tool (topology diagram), data collected from the stakeholder interviews, and any existing application architecture documents. A sample on-premise application architecture is depicted below.



Outcomes of an MRAP Exercise

Once the migration experts complete their analysis of the application with various data points collected, they will form a migration strategy for the application. And it starts with building a business case with both financial and non-financial views. Below is the comprehensive list of intelligence developed for any application considered for cloud migration.

Business Case (financial)	Migration Strategy	To-Be Cloud Architecture
Business Case (non-financial)	Migration Roadmap	Futuristic Cloud Architecture
Cloud Migration Decision: go / no go	Migration Scope (RACI Matrix)	Modernization Recommendations
Target Cloud Fitment Report	Risks & Dependencies	Cloudability Index
TCO Analysis	Out of Scope Deliverables	Modernization Index

Business Case

A business case built for an application should establish an unbiased and compelling reason when cloud migration is considered for an application. The business case will decide if an application should migrate to the cloud. And for us to arrive at this conclusion, the business case is usually built with 2 flavours - financial and non-financial. The financial part of the business case will argue the cost-benefit the organization would achieve by moving to the cloud while the non-financial will focus on business and technology benefits that the application would achieve by adopting cloud.

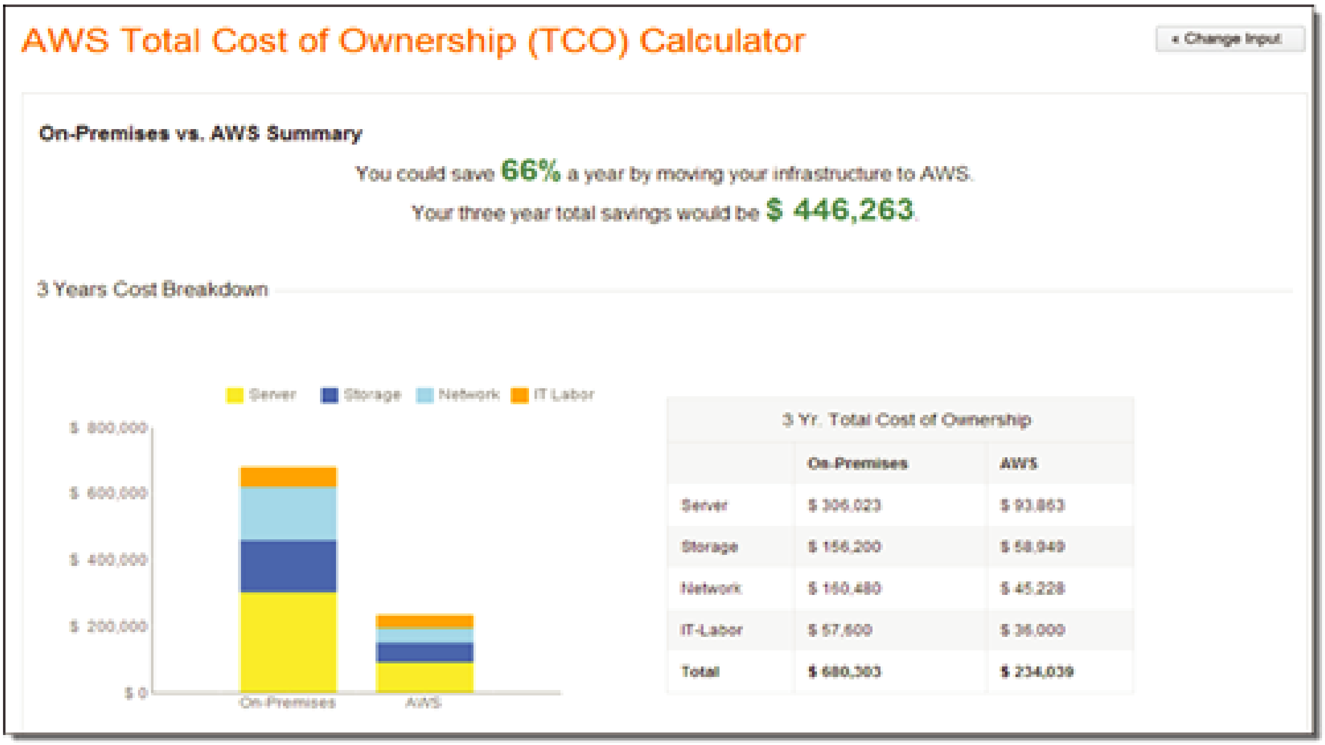
The below decision matrix is commonly applied to the business case when deciding on cloud adoption.

	Financial Benifit	Business Benifit	Technology Benifit	Cloud Adoption
Business Case of an Application	✓	✓	✓	Go
	✓	✓	✗	Go
	✓	✗	✓	Go
	✓	✗	✗	Go
	✗	✓	✓	Go
	✗	✓	✗	Go
	✗	✗	✓	No-Go
	✗	✗	✗	No-Go

The MRAP report will also recommend the target cloud platform that best suits the application provided the application has passed the business case for cloud adoption. If the target cloud has already been decided, could be an organization's commitment to a specific cloud provider or a strategic decision by the CIO, then this part could be skipped.

The TCO (Total Cost of Ownership) analysis is one of the key influencing factors for the business case of cloud adoption. By default, the expectation from the business is that cloud adoption will reduce their IT overhead cost in managing the application in the on-premise infrastructure. While the cost savings expectations cannot be met in most cases when we consider a short-term TCO gain, in the long-term the cloud does prove to be cost-efficient.

A sample TCO calculation summary (an AWS specific example) is presented below.



AWS Total Cost of Ownership (TCO) Calculator

On-Premises vs. AWS Summary

You could save 66% a year by moving your infrastructure to AWS.

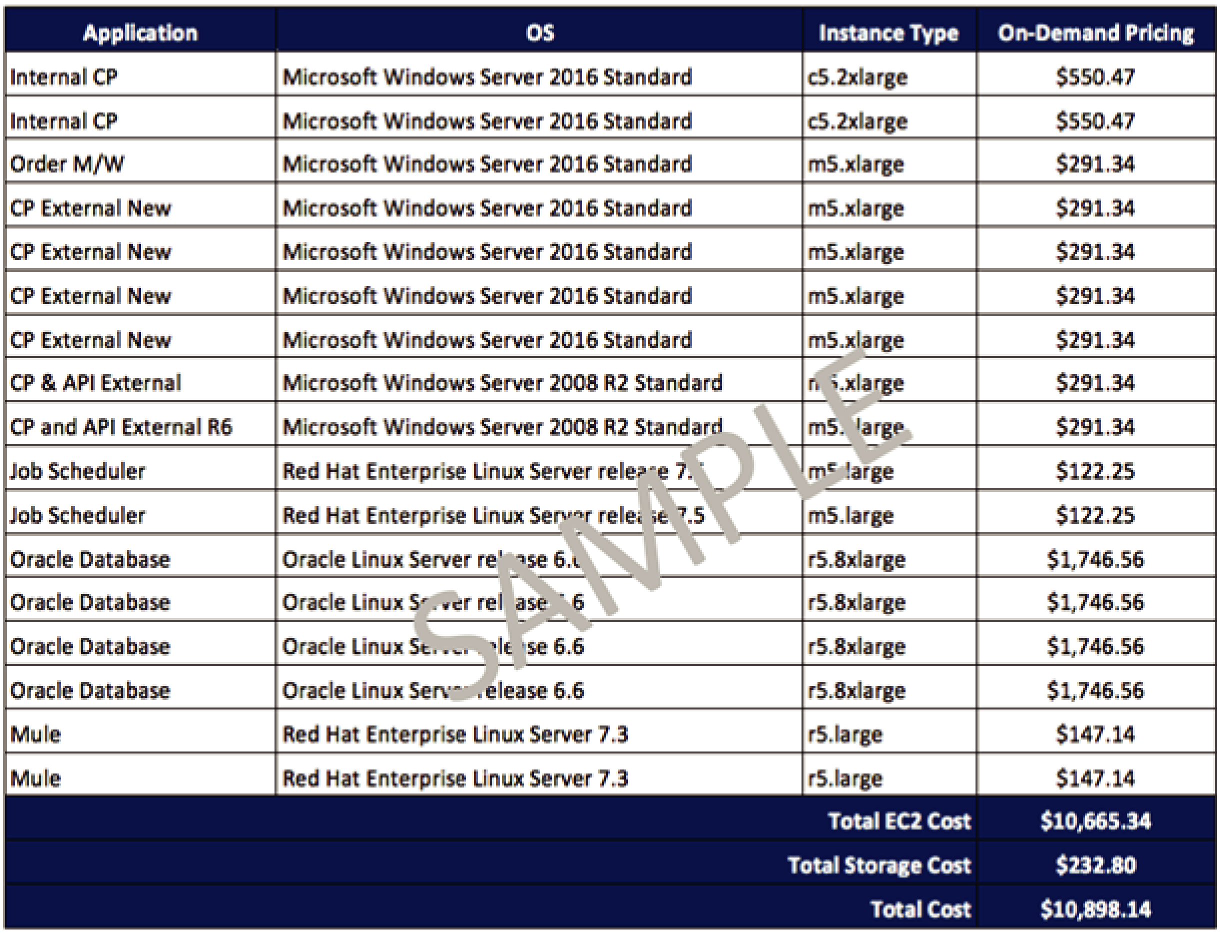
Your three year total savings would be $ 446,263.

3 Years Cost Breakdown

3 Yr. Total Cost of Ownership

	On-Premises	AWS
Server	$ 306,023	$ 93,863
Storage	$ 156,200	$ 58,049
Network	$ 160,480	$ 45,228
IT-Labor	$ 57,600	$ 36,000
Total	**$ 680,303**	**$ 234,039**

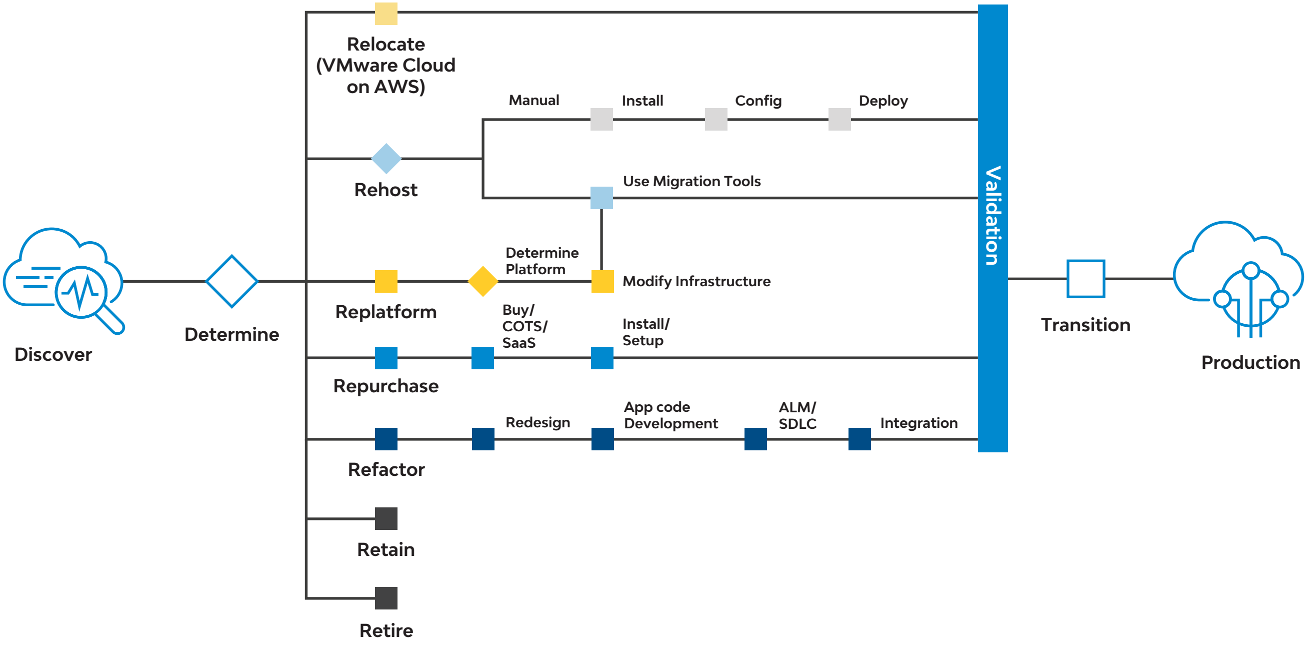
And a detailed cost calculation sheet is depicted below.



Application	OS	Instance Type	On-Demand Pricing
Internal CP	Microsoft Windows Server 2016 Standard	c5.2xlarge	$550.47
Internal CP	Microsoft Windows Server 2016 Standard	c5.2xlarge	$550.47
Order M/W	Microsoft Windows Server 2016 Standard	m5.xlarge	$291.34
CP External New	Microsoft Windows Server 2016 Standard	m5.xlarge	$291.34
CP External New	Microsoft Windows Server 2016 Standard	m5.xlarge	$291.34
CP External New	Microsoft Windows Server 2016 Standard	m5.xlarge	$291.34
CP External New	Microsoft Windows Server 2016 Standard	m5.xlarge	$291.34
CP & API External	Microsoft Windows Server 2008 R2 Standard	m5.xlarge	$291.34
CP and API External R6	Microsoft Windows Server 2008 R2 Standard	m5.xlarge	$291.34
Job Scheduler	Red Hat Enterprise Linux Server release 7.5	m5.large	$122.25
Job Scheduler	Red Hat Enterprise Linux Server release 7.5	m5.large	$122.25
Oracle Database	Oracle Linux Server release 6.6	r5.8xlarge	$1,746.56
Oracle Database	Oracle Linux Server release 6.6	r5.8xlarge	$1,746.56
Oracle Database	Oracle Linux Server release 6.6	r5.8xlarge	$1,746.56
Oracle Database	Oracle Linux Server release 6.6	r5.8xlarge	$1,746.56
Mule	Red Hat Enterprise Linux Server 7.3	r5.large	$147.14
Mule	Red Hat Enterprise Linux Server 7.3	r5.large	$147.14
		Total EC2 Cost	$10,665.34
		Total Storage Cost	$232.80
		Total Cost	$10,898.14

If there is a business benefit by moving to the cloud, then the TCO analysis is usually ignored even if the cost projection on the cloud is higher than the current on-premise one. For eg, I was advising a large payment gateway company who was gearing up for a massive sales in India. Their core MySQL database runs in a large on-premise server and they faced few downtimes during the last year's sale. So after carefully analyzing the options, I recommended them to move to AWS Aurora MySQL with the as-is schema as they had less than 60 days for the sale period to start. Since there was not enough time for database performance optimization and rewriting the data storage and retrieval logic, migrating their core database as-is to a cloud-based high-performance database was the best option. While the cost of running this large database on AWS Aurora was higher than their original spend on the on-premise server, the business was hugely benefited as there was no glitch to the application performance and zero downtime during the entire 2018 sale season. The database on the cloud could scale up to as high as 8000 requests per second which wouldn't have been possible in their on-premise setup.

It is important to define the migration strategy that one should follow for migrating an application to the cloud. There is a popular framework called 'The 7Rs Migration Strategy'. It was 6Rs which became 7Rs with the recent addition of 'Relocate' as the new option.



Let us have a quick run-through of the 7Rs migration strategy.

Relocate	Applies primarily to VMware on the AWS scenario. VMware Cloud on AWS allows you to quickly relocate hundreds of applications virtualized on vSphere to AWS.
Rehost	In a large-scale migration, scena optimizations need to migrate and scale quickly to meet a business case, such as a data center lease termination, Rehost is followed which is an as-is migration to the cloud without any changes to adopt PaaS services on the cloud.
Replatform Refactor	This entails making a few cloud optimizations to achieve tangible benefits, without changing the core architecture of the application. Eg: MySQL on a server to Amazon RDS MySQL. Typically, refactoring (or rearchitecting) is driven by a strong business need to add features, scale, or improve performance that would otherwise be difficult to achieve in the application's existing environment. Eg: Adopting microservices like Amazon Lambda for your application.

Repurchase	This is a decision to move to a newer version of the software or purchase an entirely new solution. Eg: Moving from your on-premise customer CRM software to Salesforce.
Retain	You may have portions of your IT portfolio that you are not ready to migrate, or believe are best-kept on-premises.
Retire	Decommission or archive unneeded portions of your IT portfolio.

While the 7Rs are a good way to come up with an overall strategy, it would be prudent to lead with a modernisation approach or you risk your cloud setup turning into a legacy environment once again.

The M+M Strategy

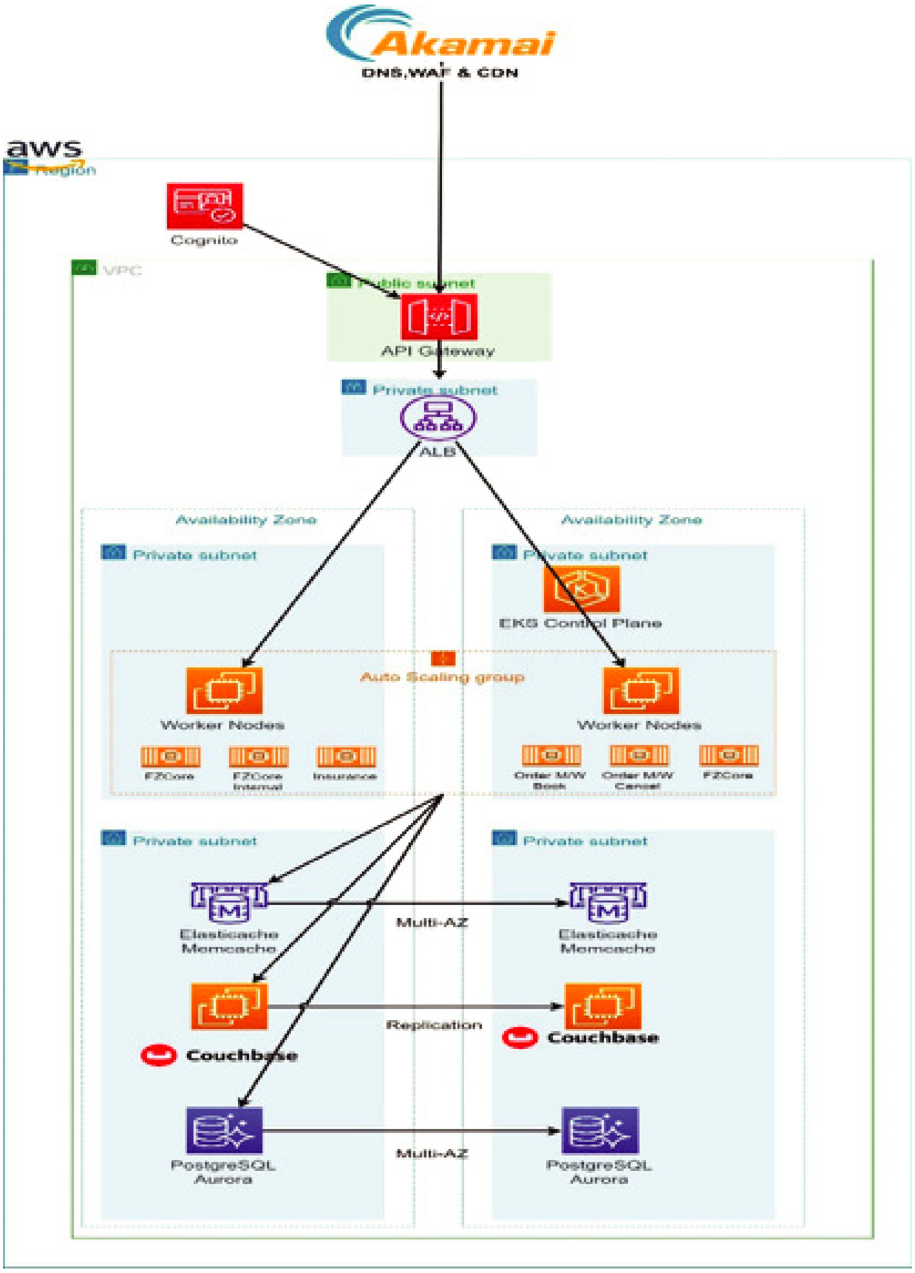
The M+M (Migrate + Modernise) Strategy, coined by us, is the most popular model followed for a modernized architecture on the cloud. The M+M strategy doesn't alienate modernization from migration activity and is included as part of the migration scope. There are 3 ways to execute the M+M strategy while migrating to the cloud.

Rehost and Modernize	• This model suits better for customers who want to move to cloud in a short duration and then continue the modernization on the cloud Eg: Migrate an application to AWS and then adopt containerization for the application on AWS using Amazon Elastic Kubernetes Service (EKS)
Refactor and Modernize	• This is probably the slowest migration model among all 7Rs as this model focuses on making the changes to the application to suit a modernized architecture on the cloud Eg: Adoption a microservice like Amazon Lambda to trigger the thumbnail creation for a video uploaded in a video streaming application
Modernize and Rehost	• Some customers define a lower degree of modernization like adopting Terraform for their applications and then migrate to the cloud Eg: Enable Terraform templates for all your applications and then move to the cloud which will give you an option to switch among multiple cloud platforms in the future

The migration strategy has its pros and cons and it is the responsibility of the cloud migration expert to come up with the strategy that best aligns with most CIO's vision on modernization and other considerations like budget, timeline, technology, etc.

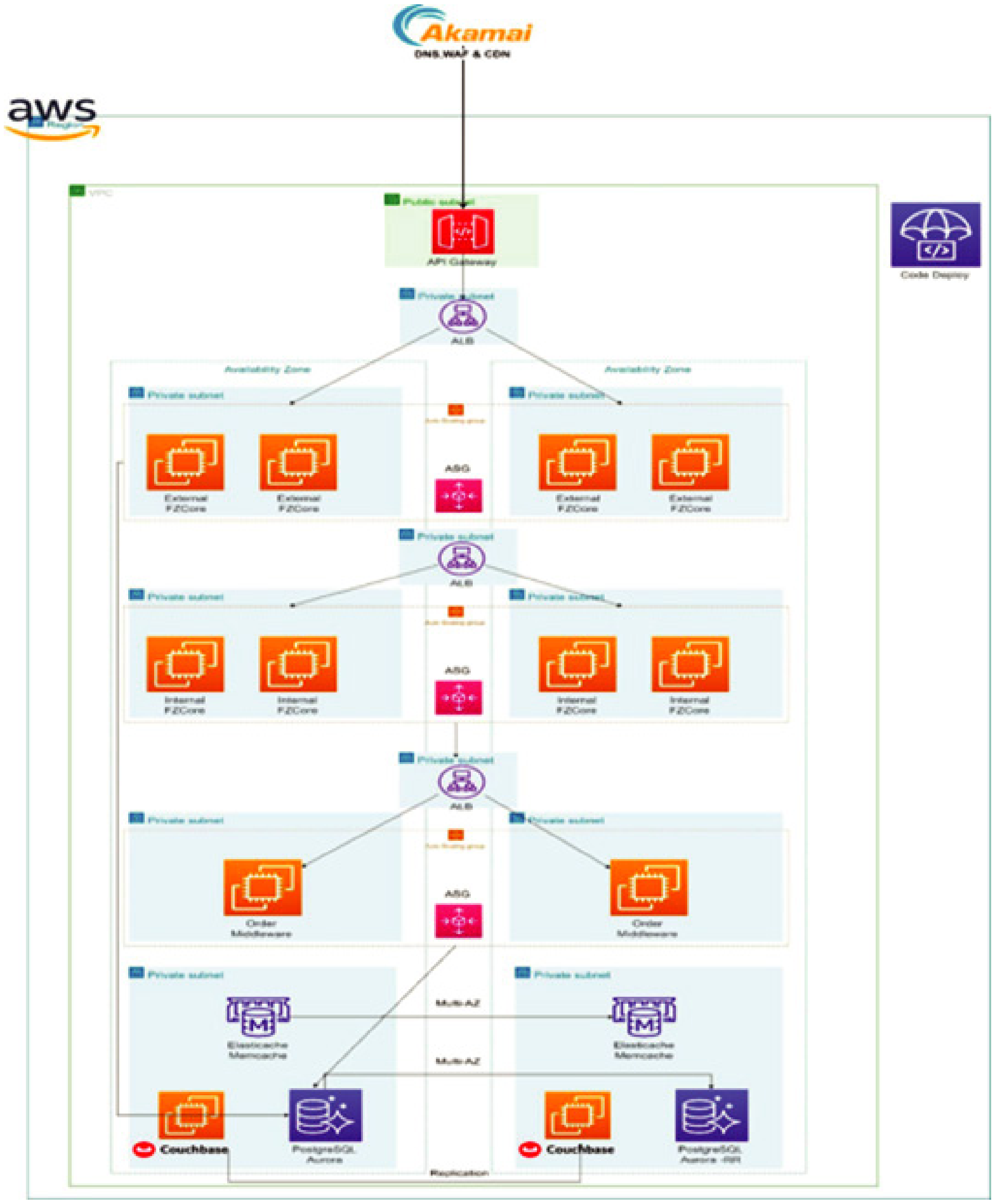
Any cloud migration expert tries to ensure that the application is migrated to the cloud with the most modernized architecture. However often, Rehost model of migration is followed owing to the budget and timeline constraints, with modernization as a follow-up activity. But designing the futuristic cloud architecture will help the migration teams and modernization teams on what is the path for future and make changes to the application accordingly.

A sample futuristic cloud architecture and modernization recommendations are depicted below.

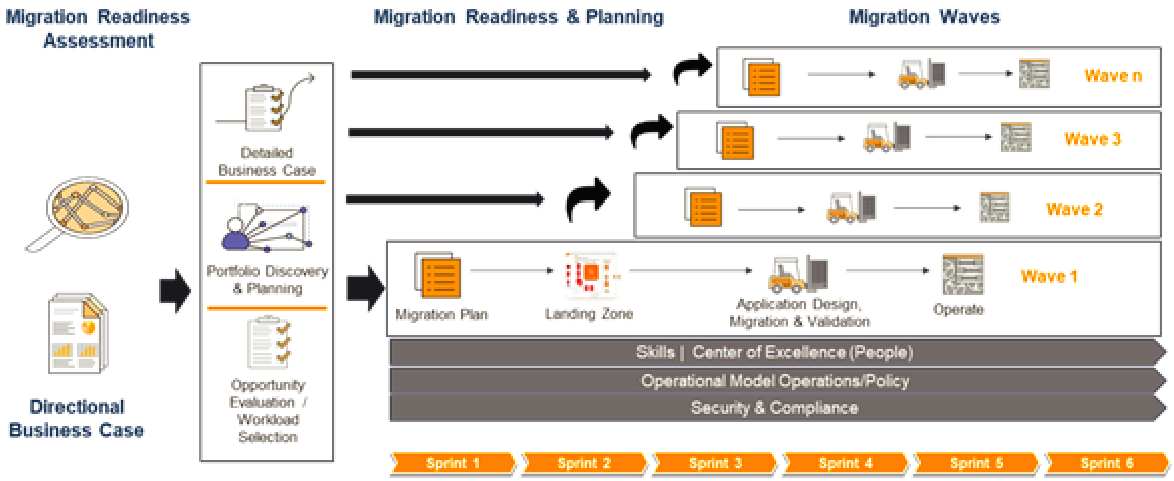


The default cloud blueprint architecture that will be designed for a Rehost model of migration. The cloud architecture will follow the Well-Architected Framework recommended by leading cloud player like AWS taking the best practices like high availability, scaling, load balancing, backups, etc into consideration.

A sample architecture design is depicted below.



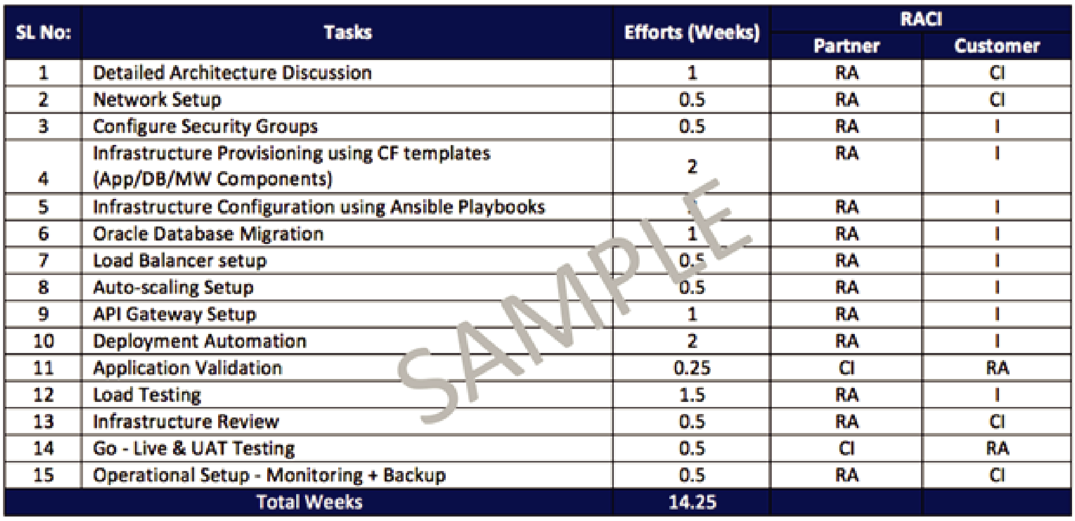
The migration roadmap defines the order in which the applications should be migrated to the cloud. In a large migration scenario that covers hundreds of applications and thousands of servers, the migration effort is divided into multiple waves. Migration roadmap allocates the applications under respective migration waves which helps in a planned seamless migration to the cloud.


Migration Readiness Assessment
Migration Readiness & Planning
Migration Waves
Directional Business Case
Detailed Business Case
Portfolio Discovery & Planning
Opportunity Evaluation / Workload Selection
Wave n
Wave 3
Wave 2
Wave 1
Migration Plan
Landing Zone
Application Design, Migration & Validation
Operate
Skills | Center of Excellence (People)
Operational Model Operations/Policy
Security & Compliance
Sprint 1
Sprint 2
Sprint 3
Sprint 4
Sprint 5
Sprint 6

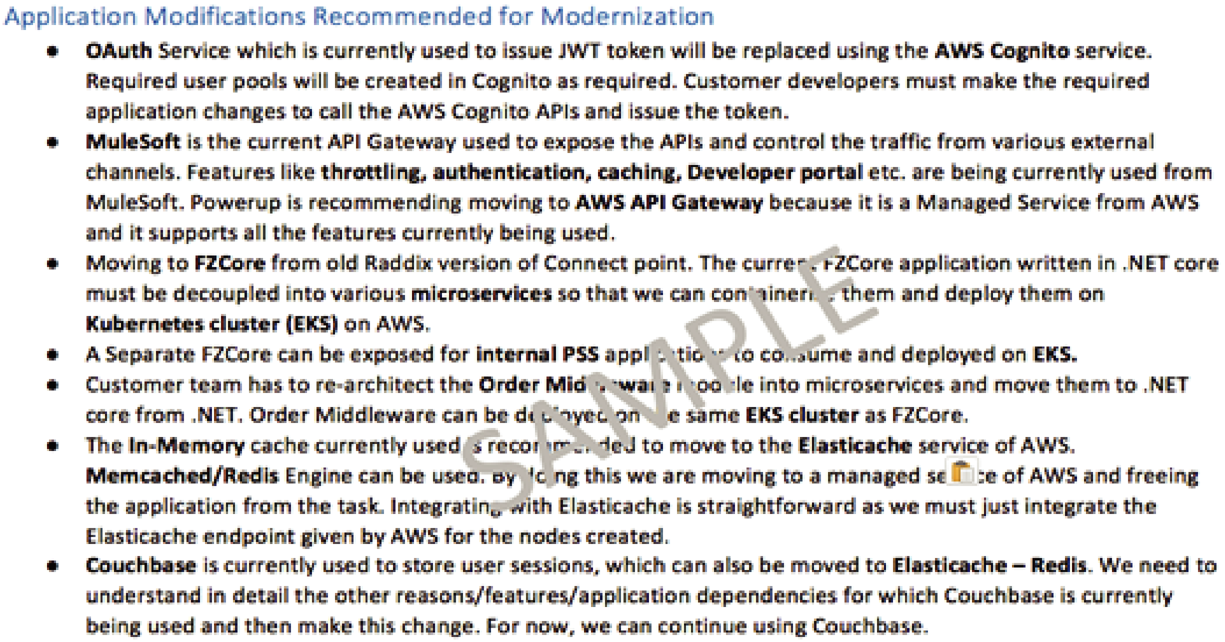
Migration Scope with RACI Matrix

The migration scope is where the cloud migration experts spend additional effort as this will define the overall duration of migrating all applications to the cloud. The migration scope is defined in a highly granular manner so that the migration team can execute the migration with minimal decisions on architecture design and implementation strategies.

A sample migration scope with the RACI (Responsibility Assignment) matrix is depicted below



SL No:	Tasks	Efforts (Weeks)	RACI	
			Partner	Customer
1	Detailed Architecture Discussion	1	RA	CI
2	Network Setup	0.5	RA	CI
3	Configure Security Groups	0.5	RA	I
4	Infrastructure Provisioning using CF templates (App/DB/MW Components)	2	RA	I
5	Infrastructure Configuration using Ansible Playbooks	[illegible]	RA	I
6	Oracle Database Migration	1	RA	I
7	Load Balancer setup	0.5	RA	I
8	Auto-scaling Setup	0.5	RA	I
9	API Gateway Setup	1	RA	I
10	Deployment Automation	2	RA	I
11	Application Validation	0.25	CI	RA
12	Load Testing	1.5	RA	I
13	Infrastructure Review	0.5	RA	CI
14	Go - Live & UAT Testing	0.5	CI	RA
15	Operational Setup - Monitoring + Backup	0.5	RA	CI
	Total Weeks	14.25		



Application Modifications Recommended for Modernization

- **OAuth** Service which is currently used to issue JWT token will be replaced using the **AWS Cognito** service. Required user pools will be created in Cognito as required. Customer developers must make the required application changes to call the AWS Cognito APIs and issue the token.
- **MuleSoft** is the current API Gateway used to expose the APIs and control the traffic from various external channels. Features like **throttling, authentication, caching, Developer portal** etc. are being currently used from MuleSoft. Powerup is recommending moving to **AWS API Gateway** because it is a Managed Service from AWS and it supports all the features currently being used.
- Moving to **FZCore** from old Raddix version of Connect point. The current FZCore application written in .NET core must be decoupled into various **microservices** so that we can containerize them and deploy them on **Kubernetes cluster (EKS)** on AWS.
- A Separate FZCore can be exposed for **internal PSS** application to consume and deployed on **EKS.**
- Customer team has to re-architect the **Order Middleware** module into microservices and move them to .NET core from .NET. Order Middleware can be deployed on the same **EKS cluster** as FZCore.
- The **In-Memory** cache currently used is recommended to move to the **Elasticache** service of AWS. **Memcached/Redis** Engine can be used. By doing this we are moving to a managed service of AWS and freeing the application from the task. Integrating with Elasticache is straightforward as we must just integrate the Elasticache endpoint given by AWS for the nodes created.
- **Couchbase** is currently used to store user sessions, which can also be moved to **Elasticache – Redis**. We need to understand in detail the other reasons/features/application dependencies for which Couchbase is currently being used and then make this change. For now, we can continue using Couchbase.

CHAPTER 5

Cloud Migration Framework That Works

An application migration involves several steps before it reaches a steady-state on the cloud. In this chapter, I will be covering the different stages involved in migrating an application or set of applications to the cloud. Having been part of over 1000 migrations over the last decade, I am illustrating a migration framework that works universally.

Cloud migration is not just about understanding the application dependencies and migrating the underlying infrastructure to the cloud. There are a bunch of pre-migration and post-migration decisions and activities that need to be performed. Let us go over them in detail.

Pre-migration Activities	• Cloud Readiness Assessment • Landing Zone or Foundation Setup on the Cloud • Network Design • Security Guardrails Design • Defining Migration Roadmap • Mitigate Identified Migration Risks • Defining Cloud Operations and Management Model • Defining Governance Model
Migration Activities	• Rs Migration Model • Governance and Security Adherence during Migration • Performance and Load Testing • Security Hardening and Chaos Monkey Testing • UAT Testing by Customer • Cut-over Planning and Execution • Support Window Post Migration
Post-Migration Activities	• Implement Operations Model • Enable Monitoring and Alerting • Enable Support Team on Incident and Problem Management • FinOps Guidelines • Continuous Performance Improvement • Continuous Modernization

A Cloud Migration Cheat Sheet

1. Have separate teams for the below tracks so that the teams follow an agile model in cloud migration and continuous modernization. This model also enforces checks at every level on the architecture design, technology decisions, etc which increases the probability of identifying and fixing any design flaws.
   a. Cloud Assessment Track
   b. Cloud Migration Track
   c. Cloud Operations Track
   d. Cloud Modernization Track

2. Follow a central cloud migration management platform like CLIC repo to bring in high visibility and transparency across multiple teams

3. Build a Cloud Centre of Excellence internally to support the cloud migration process. I have seen a high success rate at organizations that follow the Cloud CoE approach. I will cover more about a Cloud CoE design in the following section.

4. Have your Governance & FinOps team to oversee the entire migration. These teams will act as an external auditor and reduce the chances of cost mismanagement or security loopholes during the migration phase.

5. Establish a clear chain of command in your organization so that the exception approvals are handled in a hierarchy model.

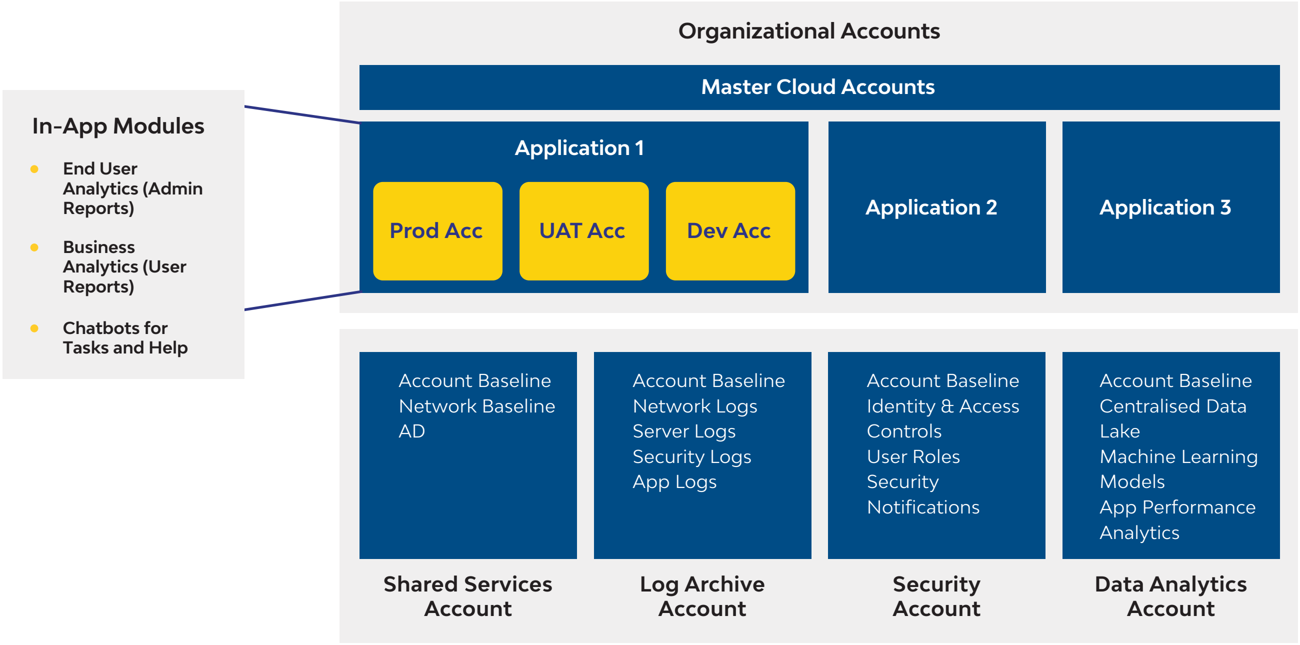
6. Impleoptimizeust program management for the migration backed by a migration management platform like CLIC repo or PPT based reports.

7. Don't optimise for performance during the migration phase if you follow Rehost (Lift and Shift) or Replatform (Lift-Transform-Shift) migration models.

8. See that the migration teams and operations teams follow a pyramid structure (covered in the Cloud CoE section) so that you don't end up being top heavy or bottom heavy. You need the right mix of architects, engineers, and specialists to execute these tracks successfully.

Importance of The Landing Zone on Cloud

The design and implementation of a landing zone and control tower for the cloud infrastructure is one important step towards designing a robust network layer and security layer for hosting the applications on the cloud. A comprehensive landing zone design (also known as cloud foundation layer) is represented below.



A well-designed landing zone has dual benefits, one helping in saving time in provisioning scalable architecture environments for multiple applications while delivering better governance.

Designing a Cloud Landing Zone Architecture

- The cloud landing zone has an overarching master cloud account which acts as the root account for all applications.
- Each application is designed as a logical layer within the master cloud account and each of these applications will have their own set of accounts that segregates the production environment from UAT & development environments.
- While the application accounts are silo-based individual accounts, there is a set of shared accounts in the cloud landing zone which improves governance and security of the entire infrastructure architecture of the application landscape.
    - Shared Services Account: The Shared Services Account is a reference for creating infrastructure shared services such as directory services including Active Directory, SSO, etc.

  - Log Archive Account: Log Archive Account contains a central repository to store the copies of all the cloud logs (access logs, error logs, config logs, etc) which allows a secure way of storing logs and avoid any tampering of evidence during an investigation.
  - Security Account: The Security Account creates audit (read-only) and admin (full-access) cross-account roles to access all individual application accounts. The intent of these roles is to be used by the security and compliance team to audit or perform emergency security operations in case of an incident.
  - Data Analytics Account: This account holds the central data lake and analytics engine including the model training and model store which will be accessed by individual applications.

- The in-app modules like end-user analytics, business analytics, and chatbots will run within the respective application environments.

What happens when you migrate without Cloud Governance in place?

Here is a true story, and I guess there is no better way to learn i.e. from other's follies.

A large e-commerce company was migrating its core e-commerce application from on-premise to Cloud. A part of this migration was a complex database migration involving Elastic Search migration from the on-premise servers to Cloud. Not unlike most organizations, this e-commerce company did not enable cloud governance during the migration, typically only considered during the steady-state management phase. So with no governance in place, the cloud team went ahead with executing the migration without adhering to any security guardrails or following a well-architected framework.

The database engineer who was leading the migration of ElasticSearch databases to Cloud decided to migrate the databases outside of the VPN connection that was established between the on-premise infrastructure and Cloud. His theory was, "The ElasticSearch migration will not take more than 24 hours, so I can migrate the database over a public IP and then close the IP post-migration. What can possibly go wrong in 24 hours?". This, as you would agree, is how a lot of migrations get done consciously ignoring any protocols in the interest of time.

However, as luck would have it, the migration tool took a bit more time than 24 hours and ran into 3 days due to unforeseen complexities on the data. Exhausted after the tedious 72 hours, they completely forgot about the public IP and moved onto other tasks. A week later, the CXO's were met with their worst nightmare, a well known Ukrainian hacker, managed to access their customers' personal information, credit card details, and more, while claiming the same with a sample post on Twitter. Long story short, the e-commerce company ended up paying a large ransom to get him to erase the hacked data.

This could have been completely avoided by enabling cloud governance which will monitor the security loopholes and best practice violations, alerting the stakeholders of any deviation. There are many similar stories where human negligence or a design error during migration has come back and hurt large organizations at a later stage in their cloud journey. So, enabling cloud governance from Day 1 is the safest way to approach cloud migration.

In fact check Point and Cybersecurity Insiders have published their global 2020 Cloud Security Report, which highlights that 60% of enterprises with proper Cloud Governance this year will experience 33% fewer security lapses.

The leading threats cited by respondents was a misconfiguration of the cloud platform (68%), up from third in 2019's survey. This was followed by unauthorized cloud access (58%), insecure interfaces (52%), and the hijacking of accounts (50%).

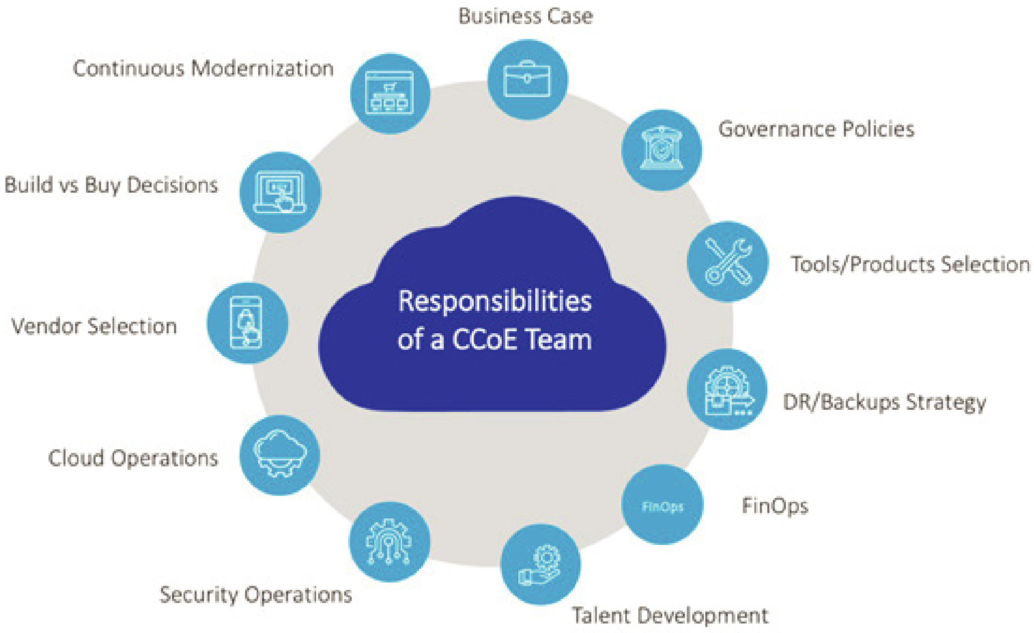
Remember, prevention is always way better than having to find a cure.

CHAPTER 6

Cloud Centre of Excellence: The Rising Trend Among Enterprises

Before we get in, a bit of history, the term Cloud Center of Excellence was allegedly introduced to the world by Stephen Orban in 2016. At the time Orban was the Global Head of Enterprise Strategy at AWS. Orban's vision for CCOE was every business with a presence in the cloud no matter what its size should have a team responsible for developing a framework for cloud operations, governing the IT infrastructure, and building out best practices throughout the business. Provide the springboard for adopting new technologies faster to better serve the business's commercial interests. But according to a recent survey, only 16 % of the organizations had a CCOE team while 47% were still working towards it.

A Cloud Centre of Excellence or CCoE is a multi-functional team of cloud specialists with a defined set of responsibilities cutting across the 6 stages of cloud adoption (as depicted in the CLIC Framework under chapter 3).



Responsibilities of a CCoE Team

While the responsibilities of a CCoE can be dynamic with a new set of responsibilities being added over a period of time as per the organization's objectives, there is a set of non-negotiable tasks that the CCoE will have to execute. They are,

- Help the organization build a strong business case for cloud adoption.
- Help the organization in selecting the right cloud platforms that suit the organization's objectives.
- Help the organization in selecting the right set of cloud management tools across assessment, migration, operations, security, governance, management tracks.
- Help the organization in preparing RFI/RFP for cloud-related requirements.
- Assist the CIO team and procurement team in vendor selection.
- Assist business teams on 'Build vs Buy' strategies for the business applications.
- Establish a governance framework for the organization's cloud ecosystem and co-own it with the operations team.
- Establish DevSecOps practice for the organization's cloud ecosystem and co-own it with the operations team.
- Establish FinOps practice and control the cloud costs.
- Establish a business continuity plan by planning backups and disaster recovery framework for the organization and co-own it with the operations team.
- Continue to explore new cloud services released and fuel the innovation charter with cloud solutions.
- Own the cloud talent development track helping the organization to be self-sufficient on cloud expertise.
- Build cloud-based proprietary platforms (IPs) for the organization and add technology assets to the organization.

5 Stages of CCoE

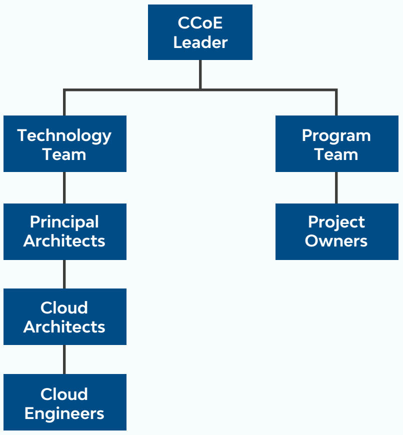
Forming a CCoE is not something that you can achieve by the sunrise. A methodical way of building the CCoE will help you carry out a trial-and-error model to arrive at the optimal CCoE structure for your organization.

Stage 1	Forming the right team of cloud specialists led by a CCoE leader
Stage 2	Identify and deliver quick wins in assessment, migration, governance, or modernization tracks
Stage 3	Obtain leadership support and receive investments to grow the CCoE

Stage 4	Build reusable templates for automation and IPs in the cloud space
Stage 5	Train, Learn, Evangelize and continue to build a strong captive cloud unit

CCoE Team Composition

Like I mentioned earlier, the team composition is the key to execution, be it in the CCoE unit or other cloud units like migration, operations, etc. Below is a recommended structure that can be considered as your Day 0 CCoE team structure.



- The CCoE leader will be aided by 2 teams -a technology team and a program team.
- The program team will run individual programs like innovation, FinOps, governance, etc.
- The program management team will also own the talent development track across the organization.
- The cloud technology reduces the gap between two technology lines (like governance & security or DevOps and SecOps), thus 2-3 multi-functional principal architects will be able to lead the technology part of CCoE.
- The principal architects will be supported by cloud architects and cloud engineers with different specializations like DevOps, security, networking, cost control, etc.
- The CCoE team's responsibilities will continue to grow which would result in a larger branched out CCoE team in the future date.

CHAPTER 7

The 4 Ops: DevOps, FinOps, SecOps, CloudOps

The operations in the cloud have evolved from two functions to four functions in the last few years. The 4 major ops functions that help you run efficient cloud operations fall under 2 broad categories.

Category	Ops Function
Cloud Management	● DevOps ● CloudOps
Cloud Governance	● FinOps ● SecOps

Ops Function	Responsibilities
DevOps	● Build and automate the CI/CD pipeline enabling faster release cycles and faster GTM for business. ● Adopt new technologies like containers, microservices, etc to improve the automation of the application stack on the cloud. ● Assist modernization team or carry out application modernization.
CloudOps	● Manage the cloud environment with 24*7 monitoring and management of the applications running on the cloud. ● Handle service requests for provisioning infrastructure and incident/problem requests to fix the application/cloud level issues.
FinOps	● Establish cost control for the cloud environment and manage the cloud spend by carrying out a cost. ● Establish a cost center for all business teams and application teams, helping them with the cloud spend data, enforcing rational use of cloud.

SecOps	• Establish security guardrails and monitor the security spectrum on the cloud on a 24*7 basis. • Be the first responder team towards security incidents with proactive and reactive monitoring of the entire security spectrum on the organization’s cloud ecosystem.

3 Stages of implementing FinOps on Cloud

FinOps enables a shift to increase an organization’s ability to understand cloud costs and make tradeoffs through a combination of systems, best practices, and culture. Achieving steady-state with FinOps involves 3 stages as depicted below.

Inform

Detailed Assessment of Cloud Assets

- **Understand Budget Allocation**
- **Industry and Peer Level Benchmarking**
- **Identify Optimization and Improvement Areas**

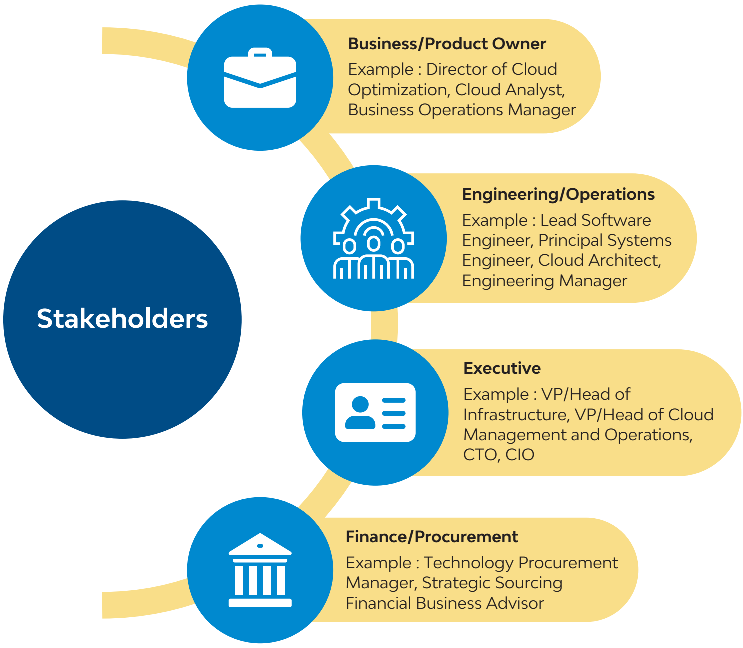
Optimize

- **Execute 9-Step Cost Optimization Process**
- **Set Thresholds and Enable Alerts**
- **Recommend Application Architecture Changes**

Operate

- **Continuous Tracking of Costs At Resource Level**
- **Cloud Governance for Pro-active Cost Control**

Structuring of FinOps teams



Stakeholders

Business/Product Owner
Example : Director of Cloud Optimization, Cloud Analyst, Business Operations Manager

Engineering/Operations
Example : Lead Software Engineer, Principal Systems Engineer, Cloud Architect, Engineering Manager

Executive
Example : VP/Head of Infrastructure, VP/Head of Cloud Management and Operations, CTO, CIO

Finance/Procurement
Example : Technology Procurement Manager, Strategic Sourcing Financial Business Advisor

Principles

1 Teams need to collaborate

2 Businedd Value of cloud drives decisions

3 Everyone takes ownership for their cloud Usage

4 FinOps reports Should be accessible and timely

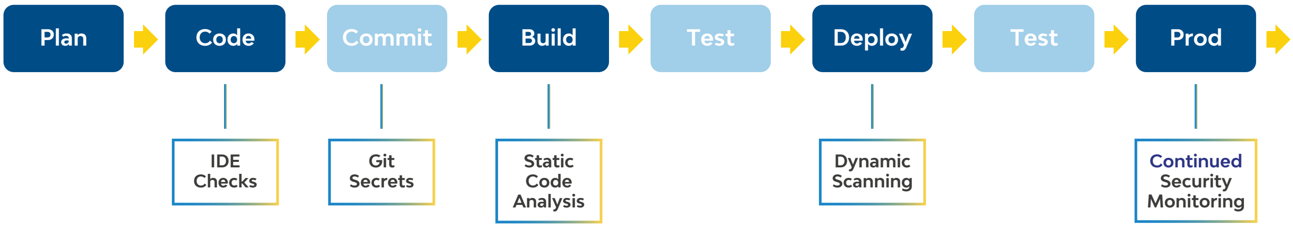
5 A centralized team drives FinOps

6 Take advantage of the variable cost model of cloud

The Evolution of DevSecOps

DevSecOps is an upcoming combination that essentially synergises DevOps with SecOps. DevSecOps function intends to design the application with the mindset that 'everyone is responsible for security'. The primary goal of this layer is to safely distribute the security decisions at speed and scale to those who hold the highest level of context.

80% of Organizations Struggle to Meet Application Delivery Requirements With Existing Infrastructure, NS1 Study Shows. In a recent study by RightScale, it was found that 84% of enterprises have adopted DevOps practices, and 30% have implemented DevOps principles across their entire organization.



Once the DevOps pipeline is established for the application (which depends on the application codebase, the purpose of the application, etc), the next step is to introduce the security checkpoint at different stages of the pipeline. These security checkpoints ensure that the coder doesn't pass on the code without completing the checkpoint and fulfilling all security needs. The baseline security checkpoints include IDE checks, static code analysis, dynamic scanning, and continued security monitoring which happens post-production.

CHAPTER 8

The Rise of Cloud Governance

Cloud Governance, simply put, is a function that will define the set of rules, checks, frameworks that help you control cloud costs, manage cloud security and progressively implement best practices on your cloud setup. IDG says that cloud governance and data security is among the top 5 priorities of CIOs in any transformation projects. The best available benchmark which helps you implement and manage cloud governance is the 'Well-Architected Framework' launched by leading hyperscaler like AWS

5 Pillars of Well-Architected Framework

Well-Architected helps cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications and workloads. 5 pillars within the Well-Architected Framework sums up the best practices that one could implement and follow in their cloud setup.

Operational Excellence	Security	Reliability	Performance Efficiency	Cost Optimization

Operational Excellence	The operational excellence pillar focuses on running and monitoring systems to deliver business value, and continually improving processes and procedures. Key topics include automating changes, responding to events, and defining standards to manage daily operations.
Security	The security pillar focuses on protecting information and systems. Key topics include confidentiality and integrity of data, identifying and managing who can do what with privilege management, protecting systems, and establishing controls to detect security events.
Reliability	The reliability pillar focuses on ensuring a workload performs its intended function correctly and consistently when it's expected to. A resilient workload quickly recovers from failures to meet business and customer demand. Key topics include distributed system design, recovery planning, and how to handle change.

Performance Efficiency	The performance efficiency pillar focuses on using IT and computing resources efficiently. Key topics include selecting the right resource types and sizes based on workload requirements, monitoring performance, and making informed decisions to maintain efficiency as business needs evolve.
Cost Optimization	The cost optimization pillar focuses on avoiding unnecessary costs. Key topics include understanding and controlling where the money is being spent, selecting the most appropriate and right number of resource types, analyzing spend over time, and scaling to meet business needs without overspending.

While these 5 pillars are widely accepted as the key construct of a well-architected framework, we are working on expanding the framework to other evolving areas of cloud architecture like containers, network, serverless, etc.

How CloudEnsure Solves Cloud Governance Puzzles?

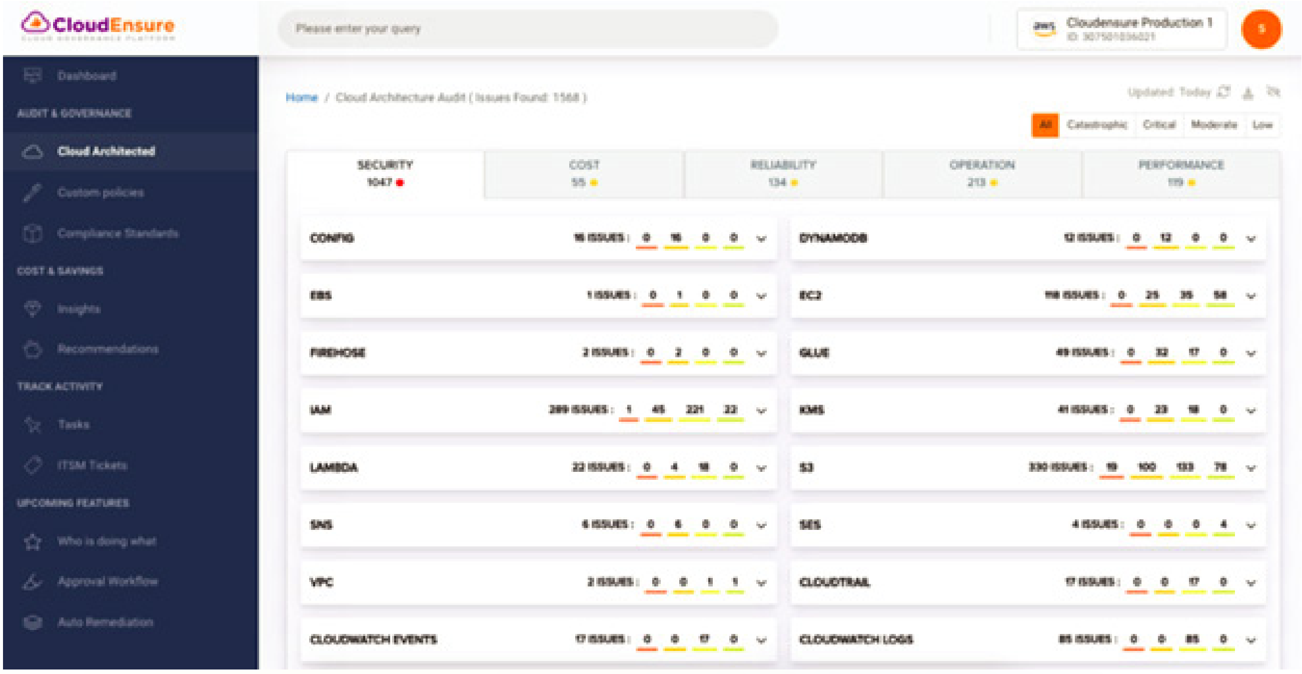
In 2018, I had a chance to interact with the CIO of one of the world's largest insurance companies. In subsequent months, we won the cloud management deal for the insurance company and helped them manage a large multi-cloud platform spread across AWS & I met the CIO a year later to review our performance on the cloud management part. While the CIO was happy about how we helped them with 24*7 monitoring and incident management with proactive and reactive support, I felt he was holding back on sharing all his pain points. When probed further, he made the following statement.

"I am not convinced that my cloud environment is foolproof from the security and governance part. My team is provisioning a lot of cloud services on a continuous basis and I am not sure if they follow the best practices. I also know that I can probably run the same setup with 30% less cost but how can I get started? If only there was a single platform which I could view every night before I sleep on all these parameters, I believe I would sleep better."

This trend is prevalent even now Gartner says more than 70% of the organizations will adopt cloud governance tools by 2025. In case of a large cloud adoption journey, CIOs are content when they see the first 25% of their applications move to the cloud, be it through the organic migration route or through the RFP route. But the real challenge begins then. We often see the cloud spend and security configurations don't go as planned and result in huge governance lapses even before the entire migration gets completed.

These scenarios triggered an idea in me to create a cloud governance platform that can monitor and report multi-cloud environments for security, cost, and best practice architecture design. We built the product and helped several large cloud customers including the above-mentioned insurance customer with automated cloud governance audits. With the introduction of Well-Architected Framework by AWS in early 2019, we adopted the 5-pillar theme onto our platform and rebranded it as the now successful autonomous cloud governance platform - CloudEnsure. Today the product has evolved to handle over 1500 checks across all 3 major cloud platforms and has autonomous remediation features too.

You can learn more about CloudEnsure at www.cloudensure.io.



Home / Cloud Architecture Audit (Issues Found: 1568)

SECURITY	COST	RELIABILITY	OPERATION	PERFORMANCE
1047 ●	55 ●	134 ●	213 ●	119 ●

CONFIG	16 ISSUES :	0	16	0	0
EBS	1 ISSUES :	0	1	0	0
FIREHOSE	2 ISSUES :	0	2	0	0
IAM	289 ISSUES :	1	45	221	22
LAMBDA	22 ISSUES :	0	4	18	0
SNS	6 ISSUES :	0	6	0	0
VPC	2 ISSUES :	0	0	1	1
CLOUDWATCH EVENTS	17 ISSUES :	0	0	17	0
DYNAMODB	12 ISSUES :	0	12	0	0
EC2	118 ISSUES :	0	25	35	58
GLUE	49 ISSUES :	0	32	17	0
KMS	41 ISSUES :	0	23	18	0
S3	330 ISSUES :	19	100	133	78
SES	4 ISSUES :	0	0	0	4
CLOUDTRAIL	17 ISSUES :	0	0	17	0
CLOUDWATCH LOGS	85 ISSUES :	0	0	85	0

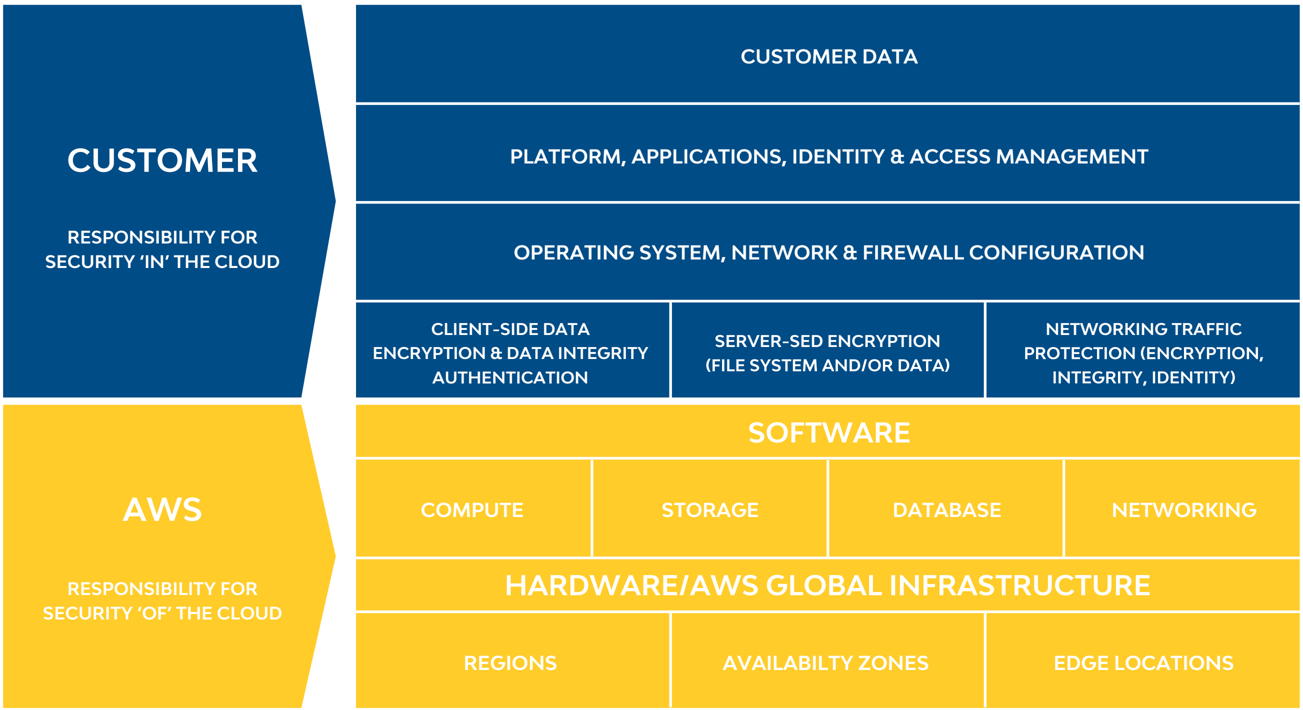
CHAPTER 9

A Deep Dive on Cloud Security

Enterprise Security is a vast & complex subject in itself, a survey shows that 59% of organizations expect their cloud security budget to increase over the next 12 months. On average, organizations allocate 27% of their security budget to cloud security. But thanks to the public cloud platforms, the infrastructure component of cloud security is simplified with cloud-native security services. In this chapter, I would be covering the base security framework which every organization should have. I will also be sharing some real case studies which show how some basic security enablement mistakes can cost a fortune for large organizations.

Security is a Shared Responsibility

Security is a shared responsibility between the cloud providers and their customers. In a few cases, the customer will share their responsibilities with a cloud consulting vendor. Below is how AWS puts across the security responsibilities in a public cloud environment scenario



CUSTOMER

RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION	SERVER-SED ENCRYPTION (FILE SYSTEM AND/OR DATA)	NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

AWS

RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD

SOFTWARE

COMPUTE	STORAGE	DATABASE	NETWORKING

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS	AVAILABILTY ZONES	EDGE LOCATIONS

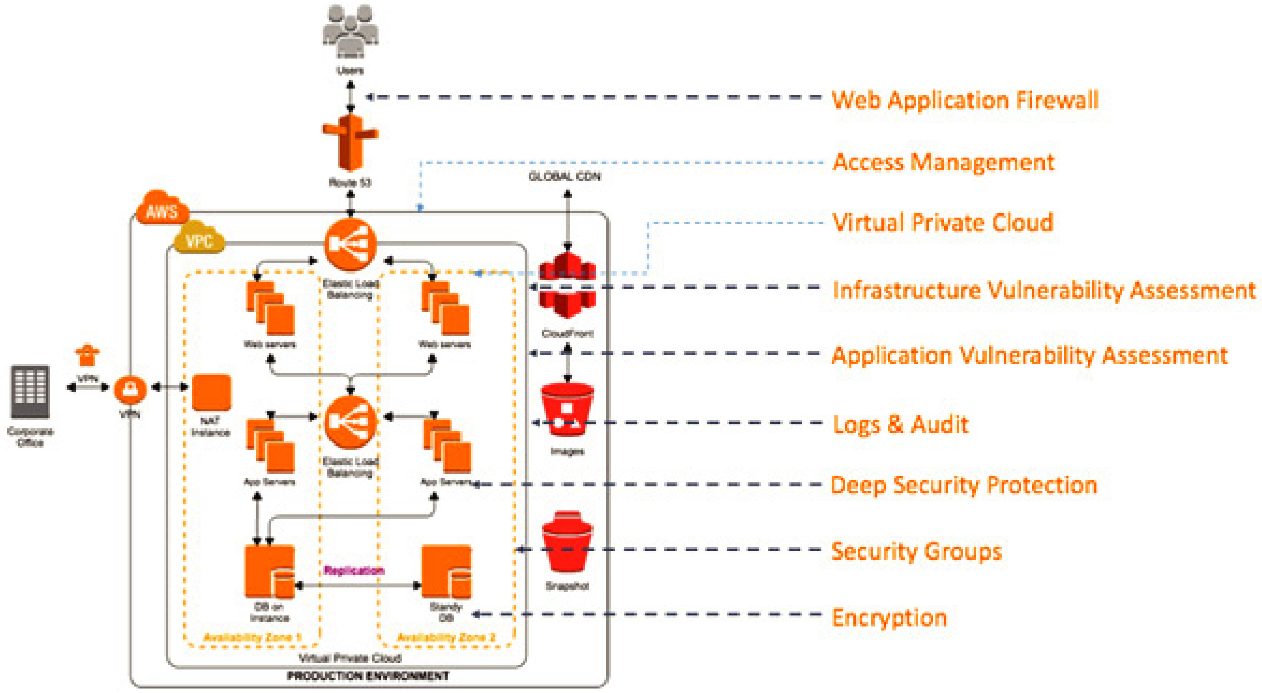
Let's see the roles played by the teams across 3 control levels.

1. Inherited Controls – Controls which a customer fully inherits from AWS.
   - Physical and Environmental controls
2. Shared Controls – Controls which apply to both the infrastructure layer and customer layers, but in completely separate contexts or perspectives. In shared control, AWS provides the requirements for the infrastructure and the customer must provide their own control implementation within their use of AWS services. Examples include:
   - Patch Management – AWS is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest OS and applications.
   - Configuration Management – AWS maintains the configuration of its infrastructure devices, but a customer is responsible for configuring their own guest operating systems, databases, and applications.
   - Awareness & Training - AWS trains AWS employees, but a customer must train their own employees.
3. Customer Specific – Controls which are solely the responsibility of the customer based on the application they are deploying within AWS services. Examples include:
   - Service and Communications Protection or Zone Security which may require a customer to route or zone data within specific security environments.

So how does this translate to the security controls of an application?

If you manage to secure your applications on the cloud with the right cloud security framework, you will by and large be compliant with the security best practices for your overall cloud environment. It is important to understand the several security layers which make up for a robust security configuration for your application.

Below is a sample application architecture on AWS with 9 layers of cloud security highlighted. If you manage to secure these 9 layers or the ones which are applicable for your application use case, this would form a good base w.r.to cloud security hardening for your applications on the cloud.



Answer the following questions to self-evaluate your application's security level on the cloud.

Are you running an internet facing web application?	If yes, then you need a Web Application Firewall to mitigate DDoS.
Are you running an internet facing web application?	If yes, you should use SSL certificates to prevent MITM attacks.
Are you concerned about your firewall security, server security and other infrastructure vulnerabilities?	If yes, you should do a comprehensive infrastructure Vulnerability Assessment & Penetration Testing (VAPT) exercise to identify these vulnerabilities and fix them.
Are you concerned about the health of your application APIs and other vulnerabilities found at application level?	If yes, you should run an application VAPT (manual tests are recommended) to identify these vulnerabilities and fix them.
Do you have a large set of people accessing your AWS infrastructure directly?	If yes, they should be accessing the servers only through a VPN.
Do you have a large set of people accessing your AWS account console directly?	If yes, you must have AD/LDAP integration with their AWS access credentials in place.

Do you have a large set of people accessing your AWS account console directly?	If yes, you should enable Multi-Factor Authentication in place.
Do you want to manage access controls to your AWS set up in a better manner?	If yes, you should maintain individual AWS accounts for different setups like Prod, UAT, Dev and one for just handling user accounts.
Do you want additional protection to your servers?	If yes, you should consider Deep Security tools which provide anti-virus, anti-malware and IDS/IPS protection.
Are you looking at encryption services?	If yes, you can consider 3rd party encryption tools which can provide data encryption and key management solutions.
Do you want to track the logs to capture unauthorized provisioning of AWS services or changes done to your AWS setup?	If yes, you should enable logging mechanisms like CloudTrail and VPC flow logs.
What about cloud-native security?	Configure VPC, security groups, subnets, ports/IP blocking rules with best practices.

CHAPTER 10

Importance of Continuous Modernization on Cloud

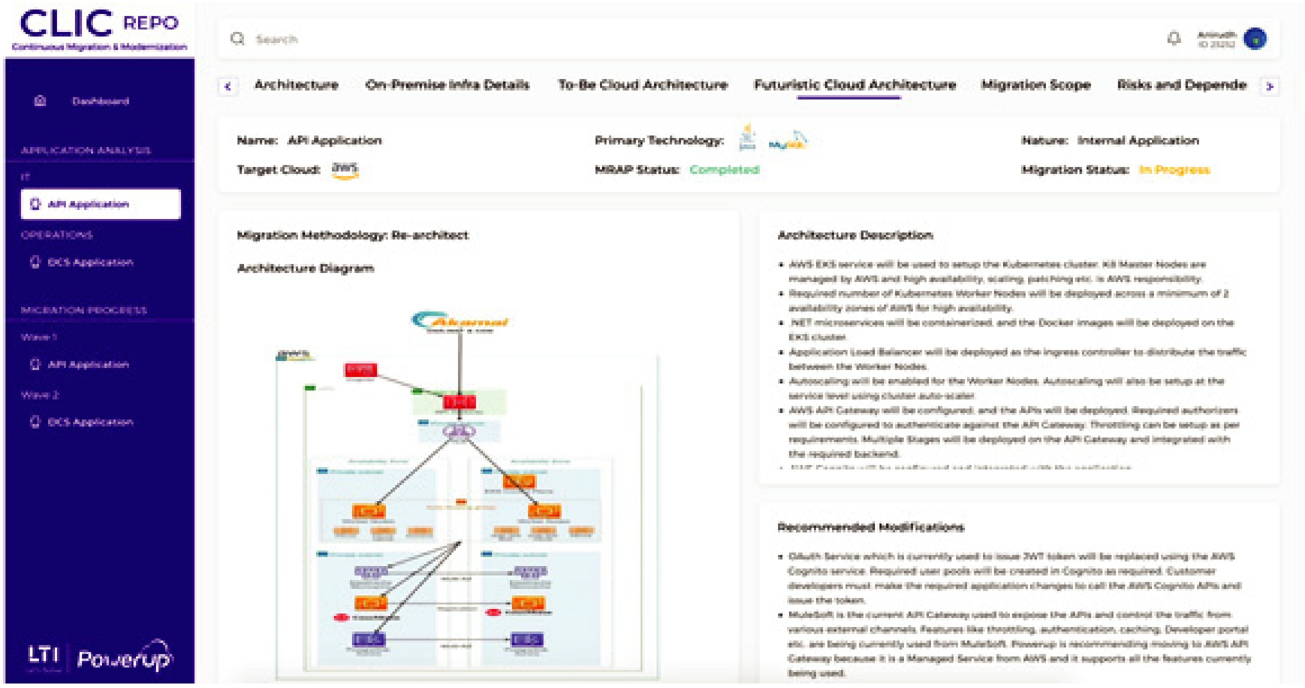
Here is what a CIO of a global financial services company quoted on modernization.

> *"I am planning to migrate close to 8,000 servers and 1200+ applications to the public cloud following the lift-shift migration model. This is a 2-year journey. But I am worried that my technology stack on the cloud will be considered the new legacy on the cloud by the time we complete the migration. I want to leverage technologies like Kubernetes, Terraform, microservices while migrating to the cloud"*

New Legacy - this is the term that the CIOs fear in the cloud era. The pace at which the cloud platforms evolve, you will have to look at a continuous modernization model to utilize the best of the cloud technology for your applications and enable businesses to fully leverage available technology giving them the edge over competitors.

Microsoft calls in incremental rationalization - An agile approach to the rationalization that properly aligns late-bound technical decisions. Many organizations move to the cloud by following the lift-and-shift (rehost) model to quickly move out of their data centers. Incremental rationalization helps these customers to build a 'modernization pod' (discussed under the Cloud CoE section) which will focus on moving these applications to a modernized architecture on cloud leveraging the new-age technology trends like serverless, containers, microservices, etc.

The CLIC repo tool built by our cloud evangelists helps large enterprise companies to execute the continuous modernization for their applications as the tool acts as the repository of all their applications on the cloud including their current architecture and the planned architecture. The application will have to go through several changes to adapt to the modern architecture on the cloud and these changes are generally advised by the cloud assessment unit or the cloud architecture design unit of the CCoE. CLIC repo also helps organizations to list the application changes required for modernization and track them effectively.



CLIC REPO
Continuous Migration & Modernization

Dashboard

APPLICATION ANALYSIS

IT

API Application

OPERATIONS

DCS Application

MIGRATION PROGRESS

Wave 1

API Application

Wave 2

DCS Application

LTI | Powerup

Search

Anirudh
ID 25252

Architecture | On-Premise Infra Details | To-Be Cloud Architecture | Futuristic Cloud Architecture | Migration Scope | Risks and Depende

Name: API Application

Target Cloud: aws

Primary Technology: Java MySQL

MRAP Status: Completed

Nature: Internal Application

Migration Status: In Progress

Migration Methodology: Re-architect

Architecture Diagram

Architecture Description

- AWS EKS service will be used to setup the Kubernetes cluster. K8 Master Nodes are managed by AWS and high availability, scaling, patching etc. is AWS responsibility.
- Required number of Kubernetes Worker Nodes will be deployed across a minimum of 2 availability zones of AWS for high availability.
- .NET microservices will be containerized, and the Docker images will be deployed on the EKS cluster.
- Application Load Balancer will be deployed as the ingress controller to distribute the traffic between the Worker Nodes.
- Autoscaling will be enabled for the Worker Nodes. Autoscaling will also be setup at the service level using cluster auto-scaler.
- AWS API Gateway will be configured, and the APIs will be deployed. Required authorizers will be configured to authenticate against the API Gateway. Throttling can be setup as per requirements. Multiple Stages will be deployed on the API Gateway and integrated with the required backend.
- AWS Cognito will be configured and integrated with the application

Recommended Modifications

- OAuth Service which is currently used to issue JWT token will be replaced using the AWS Cognito service. Required user pools will be created in Cognito as required. Customer developers must make the required application changes to call the AWS Cognito APIs and issue the token.
- MuleSoft is the current API Gateway used to expose the APIs and control the traffic from various external channels. Features like throttling, authentication, caching, Developer portal etc. are being currently used from MuleSoft. Powerup is recommending moving to AWS API Gateway because it is a Managed Service from AWS and it supports all the features currently being used.

Expert Tips: *Don't allow your cloud environment to become the 'new legacy'. Have a modernization pod to enable continuous modernization of your cloud environment.*

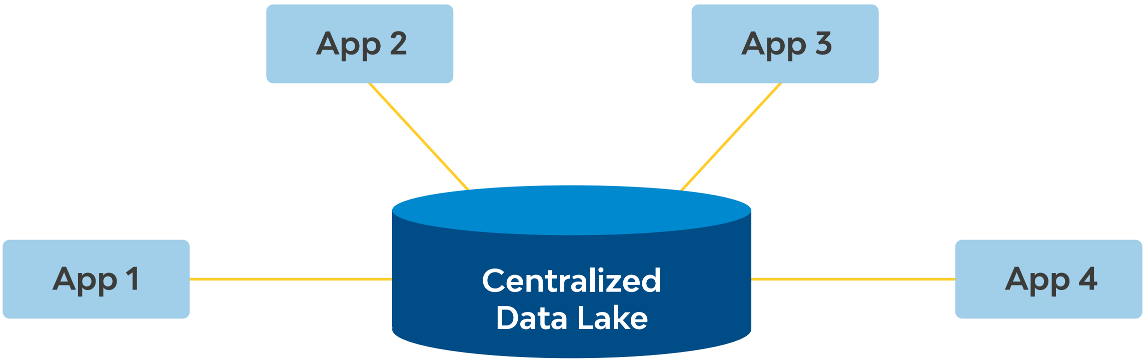
CHAPTER 11

The Cloud is Much More Than Just Hosting - Data, AI, ML, IoT

Cloud Strategy is much more than just hosting applications on the cloud. Data the core plays an integral role in a modern cloud strategy. With the continuing advancement of cloud offerings in the field of Artificial Intelligence, Machine Learning, Internet of Things, Edge Computing. Studies suggest 100% of supply chain apps will depend on augmented reality, virtual reality, blockchain, ML, and IoT. And by 2025, 100% of enterprise applications will include some form of embedded AI. Therefore defining your data strategy is important as defining your cloud adoption strategy, for the best leverage of cloud adoption.

Designing a Cloud Strategy with Data First Approach

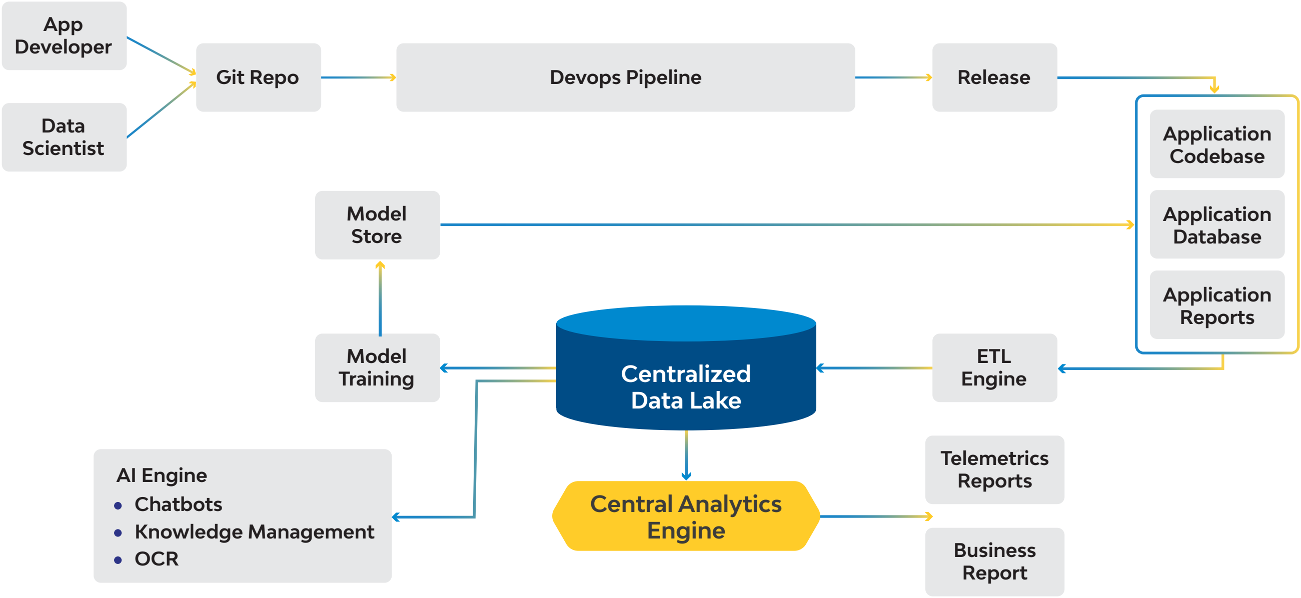
Organizations sitting on a lot of data tend to follow a data-centric design approach. I believe this is a good approach for every type of organization, irrespective of individually being data-heavy or not, as consolidated data helps in correlation and building of rich and holistic insights for any business.



The data-centric cloud design focuses on building the application architecture from a data scientist point-of-view. This will allow the architecture to streamline its data pipeline and the way the application integrates with other applications and centralized data lake of the organization. This model also focuses on integrating advanced machine learning and artificial intelligence engines with the application. This will power the in-app analytics, be it user-level analytics or business analytics for the application.

Sample Design of a Futuristic Application Architecture

Below is a futuristic application architecture designed for the cloud which leverages the data-centric design and integrated DevOps pipeline seamlessly in the overall application architecture.



How does this application architecture work?

- The code push by the App Developer or Data Scientist goes through the DevOps pipeline and upon completion of all checks, hit the release phase.
- The ETL (Extract-Transform-Load) pipeline built for the specific application will extract the data from the application, transforms the data as required, and pushes the processed data to the central data lake.
- Machine Learning models are trained by the data scientists using the cleaned data set in the central data lake and upon arriving at the right ML model, the model is published in the model store.
- The application then leverages the trained model from the model store to improve the application's efficiency in handling the business logic. (eg: Predictions, Forecasting, Recommendations, etc)
- There is a Central Analytics Engine which helps in creating two key reports,
  - Telemetric Reports: Telemetric data of an application includes the application behaviour in edge devices (eg: mobile phones, IoT devices, etc). Since the centralized data lake collects both telemetric and business data of all applications, the central analytics engine will be able to process and publish the telemetric reports of all applications in the enterprise, giving a holistic view of the edge device performance of all applications.
  - Business Reports: Business Reports on the other hand is usually generated as an in-app report. But when there is a need to collaborate data from multiple applications

(eg: CRM data with Finance data), the centralized data lake will be able to correlate the data and produce rich data insights.

AI/ML Gaining Ground in Modern Cloud Architecture

With the rise of cloud-based AI/ML platforms like Amazon and their easy integration with the data lake on respective cloud platforms, CIOs are looking at modern application architecture which can seamlessly integrate with these cutting edge technologies. The popular saying of 'Data is the new Oil' will not be of any help if you don't have the design and tools to mine them to generate rich insights.

The market is seeing some early wins in this space with the advancement of chatbots, natural language processing engines, image recognition engines, video processing algorithms, etc. In the future, almost every application will have a cognitive play and will leverage these AI/ML technologies to bring in better efficiencies to the business.

CONCLUSION

As I conclude, we should understand and accept that cloud adoption is not a one-time quick fix exercise, but rather an evolving ecosystem that grows from a solid base and yields dividends over time. Irrespective of the approach you adopt, either application first or data first, it is important to see it as a journey built on a framework that needs to be closely monitored (evolved) through its progression.

The purpose of this document was to take you through the different ways and stages that you could follow in building a successful cloud practice for your organization. As the cloud ecosystem, this document will continue to evolve and I will append with my experiences through the journeys we undertake with our clients, each providing enrichment on ways to success.

Hope you found this useful and I would like to hear from you. All the best for your cloud journey.