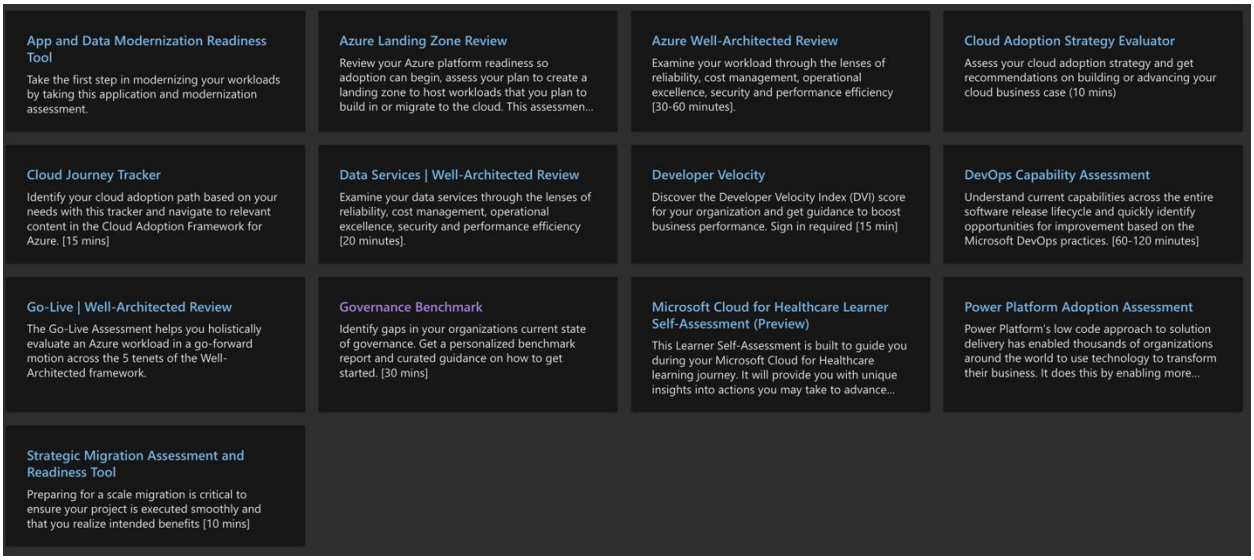
Microsoft Cloud Assessments

Available Assessments in MS:

1. App and Data Modernization Readiness
2. Azure Landing Zone Review
3. Azure Well-Architected Review
4. Cloud Adoption Strategy Evaluator
5. Cloud Journey Tracker
6. Data Services Well Architected Review
7. Developer Velocity
8. DevOps Capability Assessment
9. Go Live Well Architected Review
10. Governance Benchmark
11. Power Platform Adoption Assessment
12. Strategic Migration Assessment and Readiness
13. MS Cloud for Healthcare

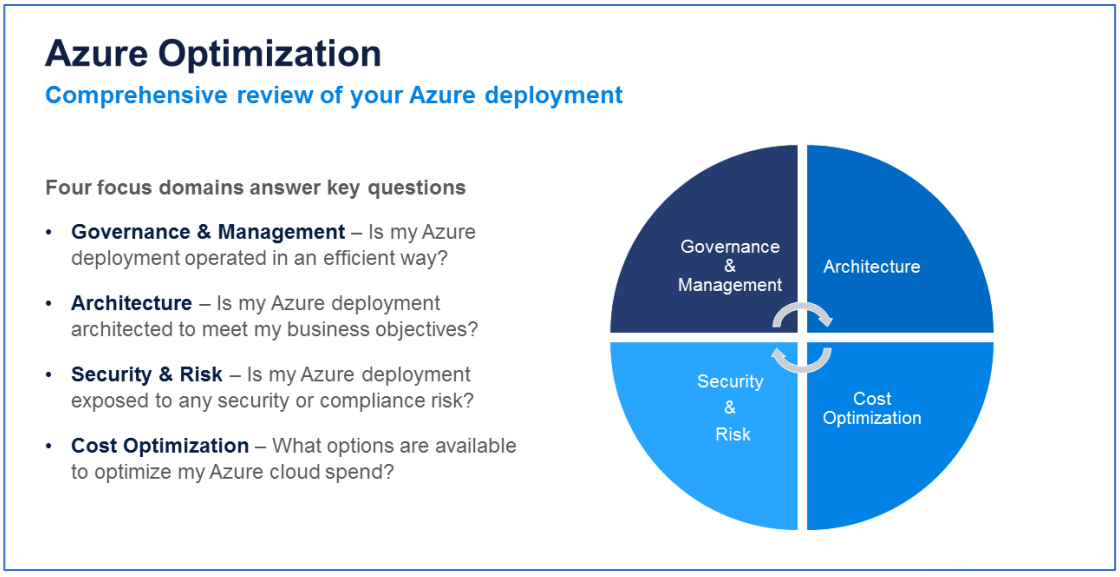


Core Pillars in Evaluation:

1. Reliability
2. Security
3. Cost
4. Operational Excellence
5. Performance

Cost Optimization Questions:

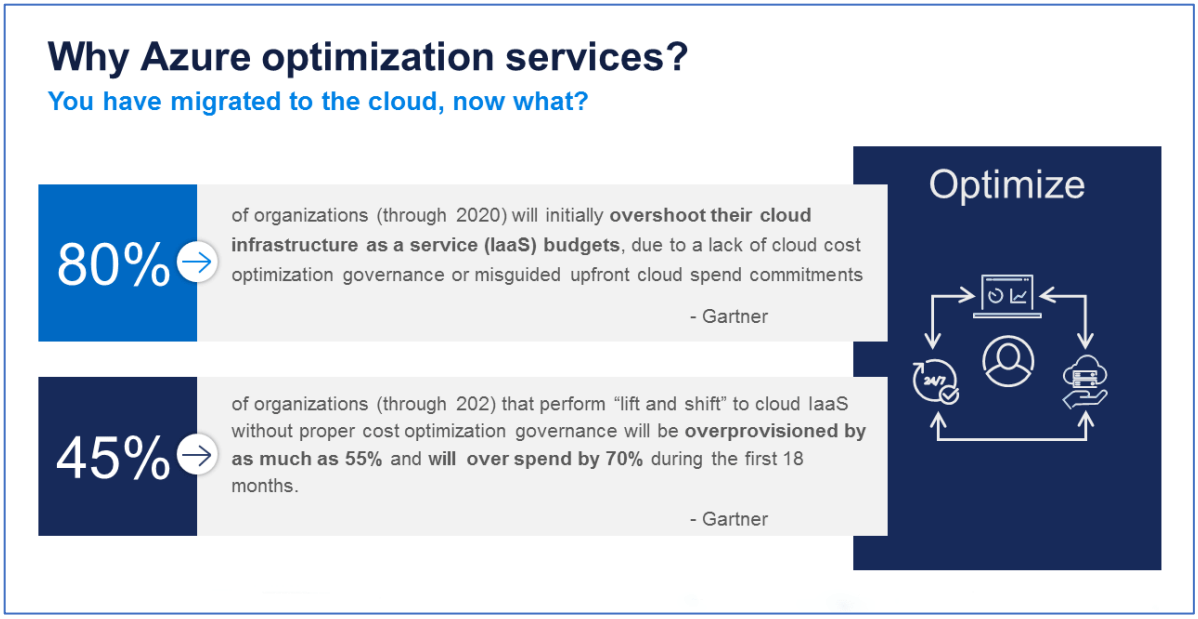
1. How are you modeling cloud costs of this workload?
2. How do you govern budgets and application lifespan for this workload?
3. How are you monitoring costs of this workload?
4. How do you optimize the design of this workload?
5. How do you ensure that cloud services are appropriately provisioned?
6. What considerations for DevOps practices are you making in this workload?
7. How do you manage compute costs for this workload?
8. How do you manage networking costs for this workload?
9. How do you manage storage and data costs for this workload?



Performance Efficiency Questions:

1. What design considerations have you made for performance efficiency in your workload?

2. Have you identified the performance targets and non-functional requirements for your workload?
3. How are you ensuring that your workload is elastic and responsive to changes?
4. How have you accounted for capacity and scaling requirements of your workload?
5. What considerations for performance efficiency have you made in your networking stack?
6. How are you managing your data to handle scale?
7. How are you testing to ensure that you workload can appropriately handle user load?
8. How are you benchmarking your workload?
9. How have you modeled the health of your workload?
10. How are you monitoring to ensure the workload is scaling appropriately?
11. What common problems do you have steps to troubleshoot in your operations playbook?



Reliability Questions:

1. What reliability targets and metrics have you defined for your application?
2. How have you ensured that your application architecture is resilient to failures?
3. How have you ensured required capacity and services are available in targeted regions?
4. How are you handling disaster recovery for this workload?
5. What decisions have been taken to ensure the application platform meets your reliability requirements?
6. What decisions have been taken to ensure the data platform meets your reliability requirements?
7. How does your application logic handle exceptions and errors?
8. What decisions have been taken to ensure networking and connectivity meets your reliability requirements?
9. What reliability allowances for scalability and performance have you made?

10. What reliability allowances for security have you made?
11. What reliability allowances for operations have you made?
12. How do you test the application to ensure it is fault tolerant?
13. How do you monitor and measure application health?

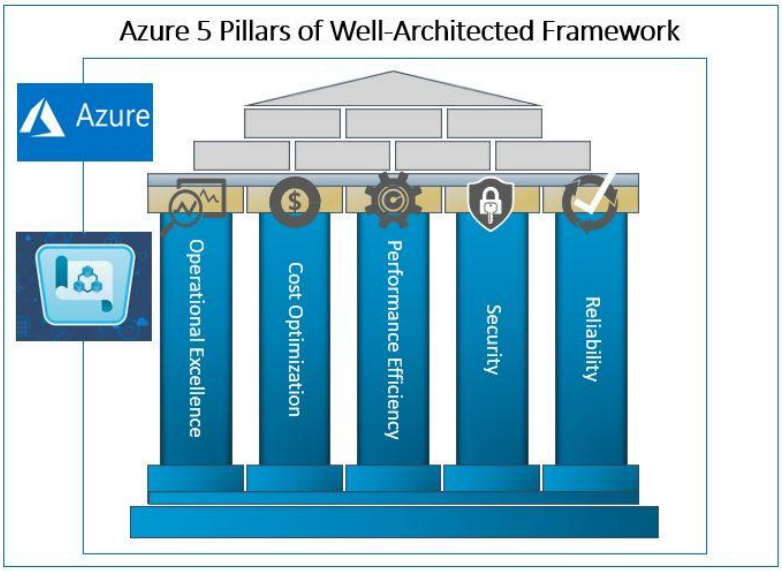
Security Questions:

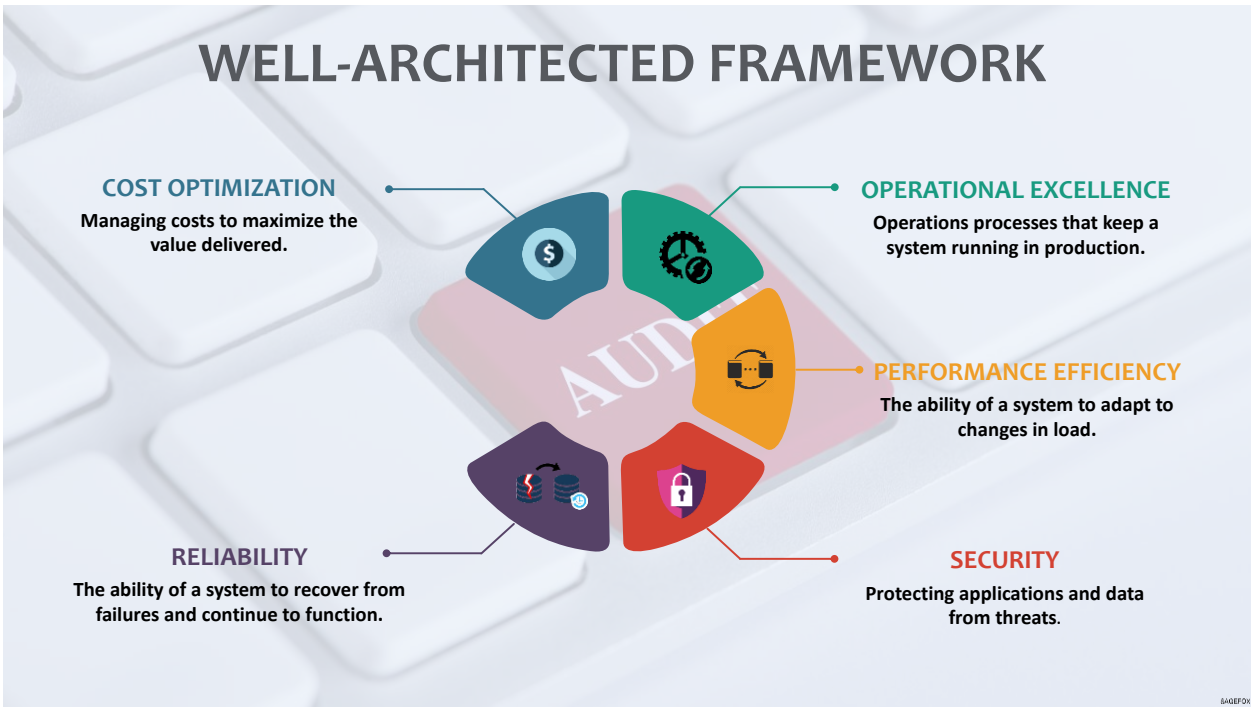
1. Have you done a threat analysis of your workload?
2. What considerations for compliance and governance did you make in this workload?
3. What practices and tools have you implemented as part of the development cycle?
4. Have you adopted a formal secure DevOps approach to building and maintaining software?
5. Is the workload developed and configured in a secure way?
6. How are you monitoring security-related events in this workload?
7. How is security validated and how do you handle incident response when breach happens?
8. How is connectivity secured for this workload?
9. How have you secured the network of your workload?
10. How are you managing encryption for this workload?
11. Are keys, secrets and certificates managed in a secure way?
12. What security controls do you have in place for access to Azure infrastructure?
13. How are you managing identity for this workload?

Operational Excellence Questions:

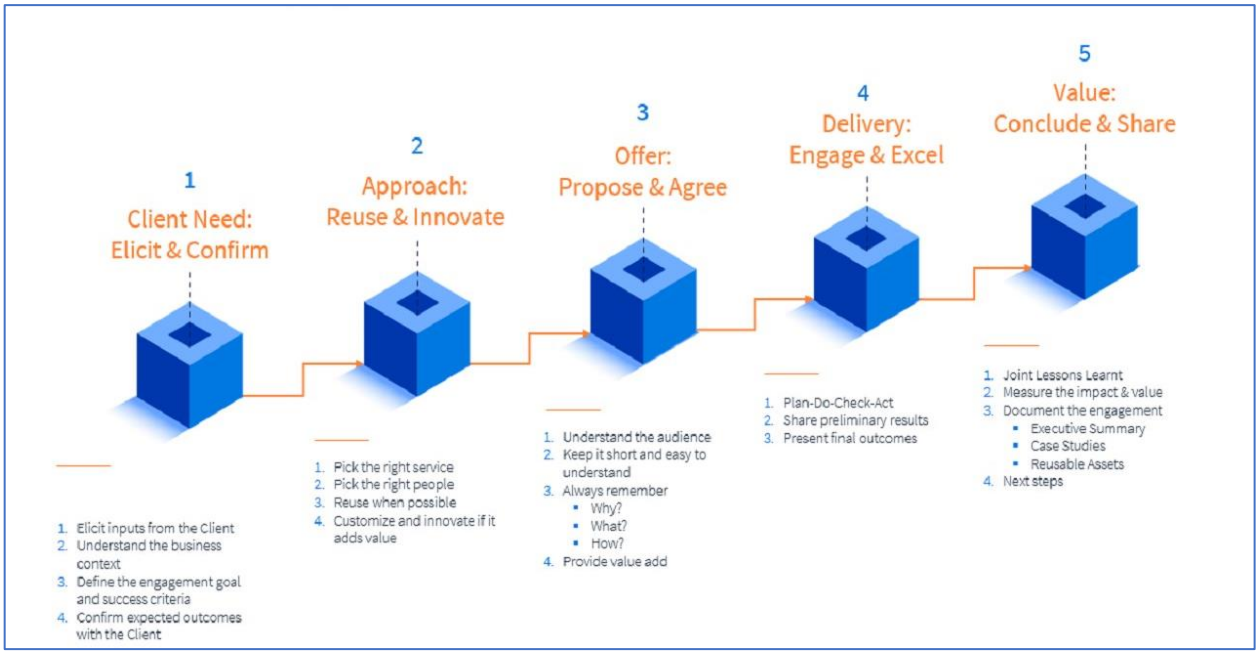
1. Have you identified and planned out the roles and responsibilities to ensure your workload follows operational excellence best practices?
2. What design considerations for operations have you made?
3. Have you defined key scenarios for your workload and how they relate to operational targets and non-functional requirements?
4. How are you monitoring your resources?
5. How do you interpret the collected data to inform about application health?
6. How do you visualize workload data and then alert relevant teams when issues occur?
7. How are you using Azure platform notifications and updates?
8. What is your approach to recovery and failover?
9. How are scale operations performed?
10. How are you managing the configuration of your workload?
11. What operational considerations are you making regarding the deployment of your workload?
12. What operational considerations are you making regarding the deployment of your infrastructure?
13. How are you managing and distributing your patches?
14. How are you testing and validating your workload?
15. What processes and procedures have you adopted to optimize workload operability?
16. What operational excellence allowances for reliability have you made?
17. What operational excellence allowances for cost have you made?
18. What operational excellence allowances for security have you made?

Well Architected Framework:

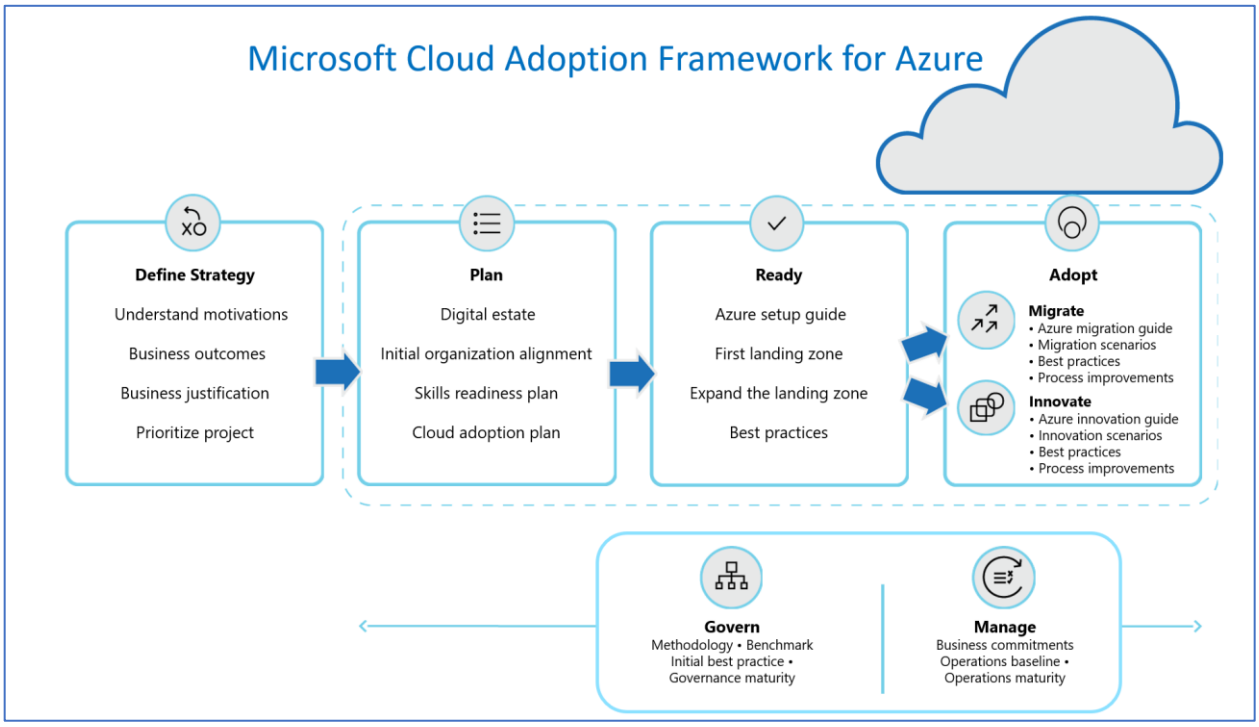




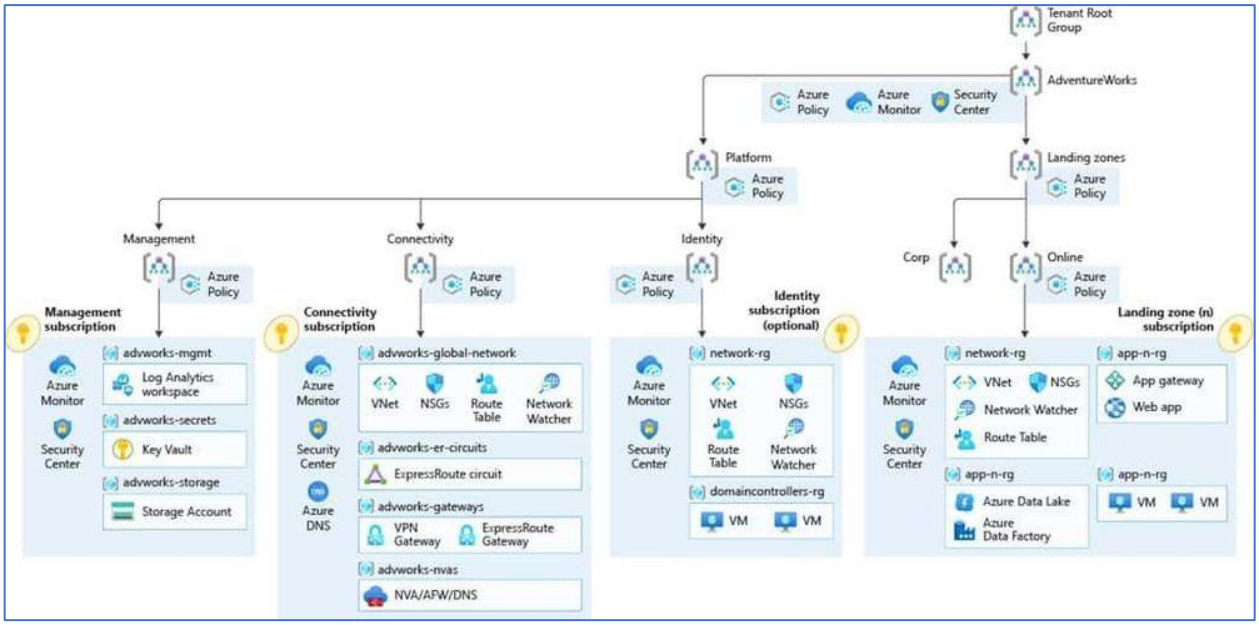
How do we do it on the Framework?



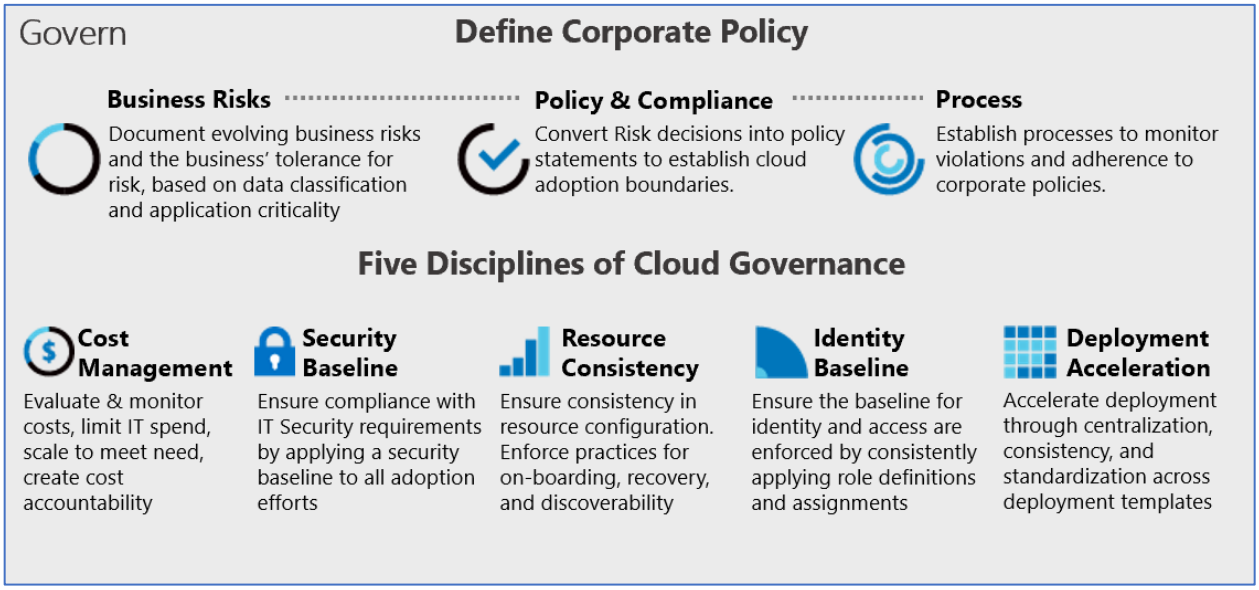
Cloud Framework used for Azure:

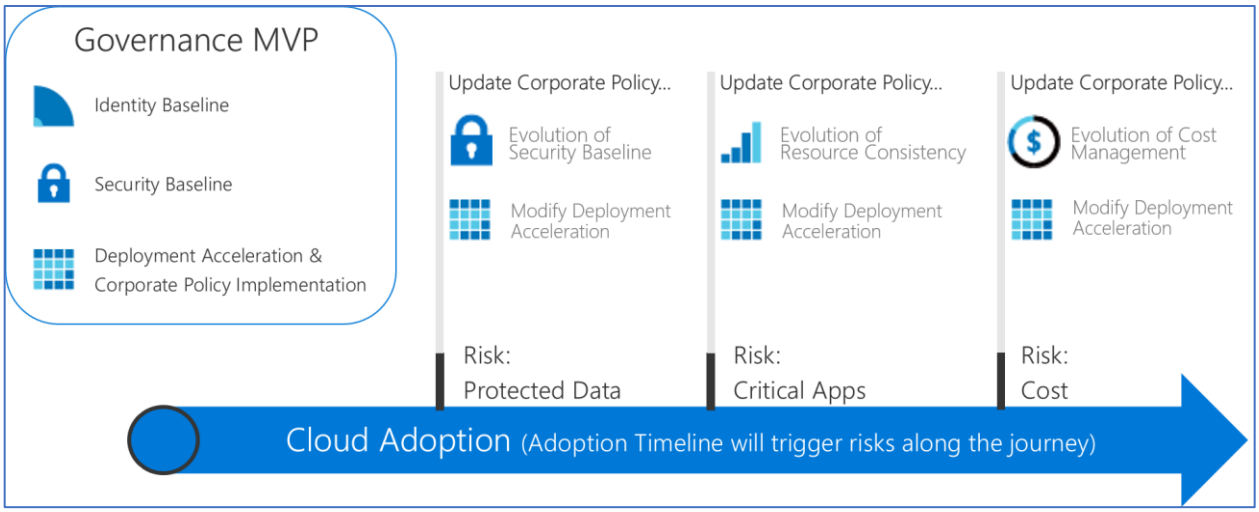


Cloud Adoption Framework:



Cloud GRC Methodology:





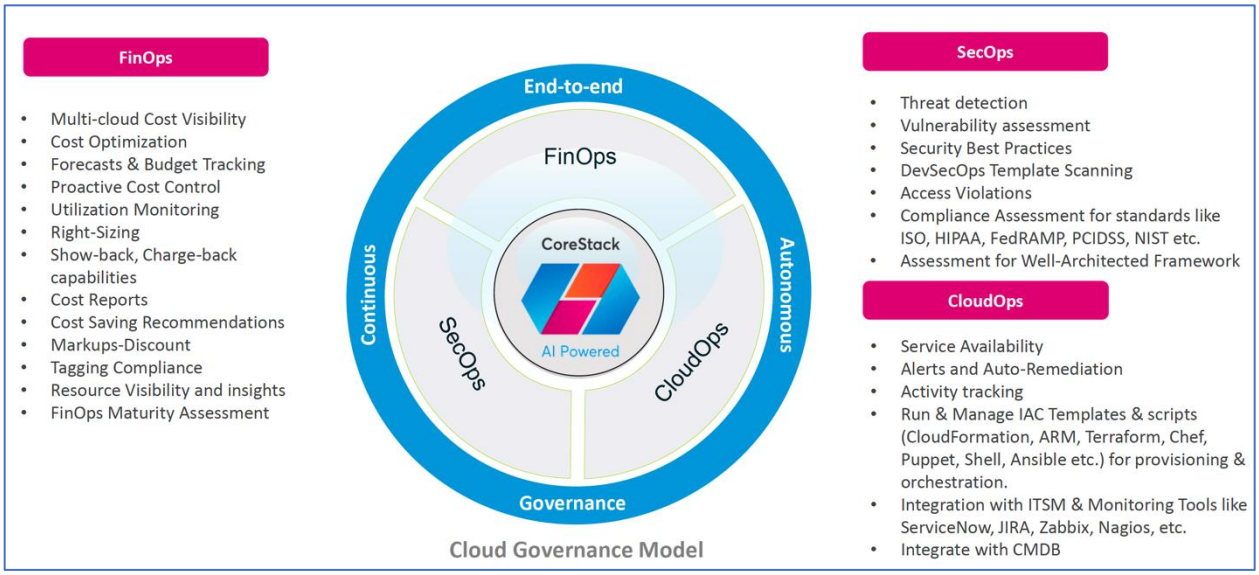
Typical Engagement Steps and Process:

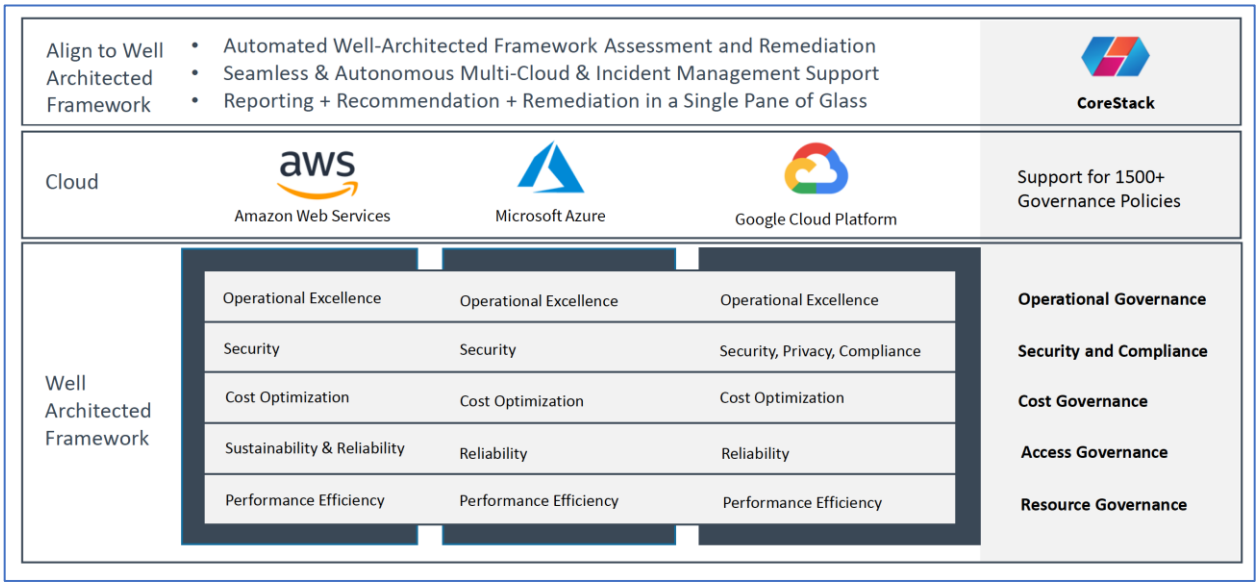
First Meeting – Discovery Call	• Validate client drivers • Confirm intrinsic value of CoreStack
Technical Deep Dive Demo	• Identify suitable use cases and in-depth demo of the product • Confirm environmental suitability
Proof of Value (POV)	• Execute real data validation of key desired outcomes of identified use cases • Customer will start testing CoreStack platform with the use cases defined.
Joint Review -Business Value Assessment	• Customer team and CoreStack team will have a joint review along with the respective stake holders and exec sponsor(s) to review the outcome and define next steps of business engagement
Final business case 'echo back' & POV evidence to customer	• Confirm technical validation and adoption • Validate business justification and formulate next steps and agreement for joint success plan
Commercial Discussion & Contract Signing	• Commercial proposal and contract signing • Enablement and adoption during rollout
Joint Success Plan EXECUTE	• Deliver services based on Joint Success Plan • Regular progress reviews

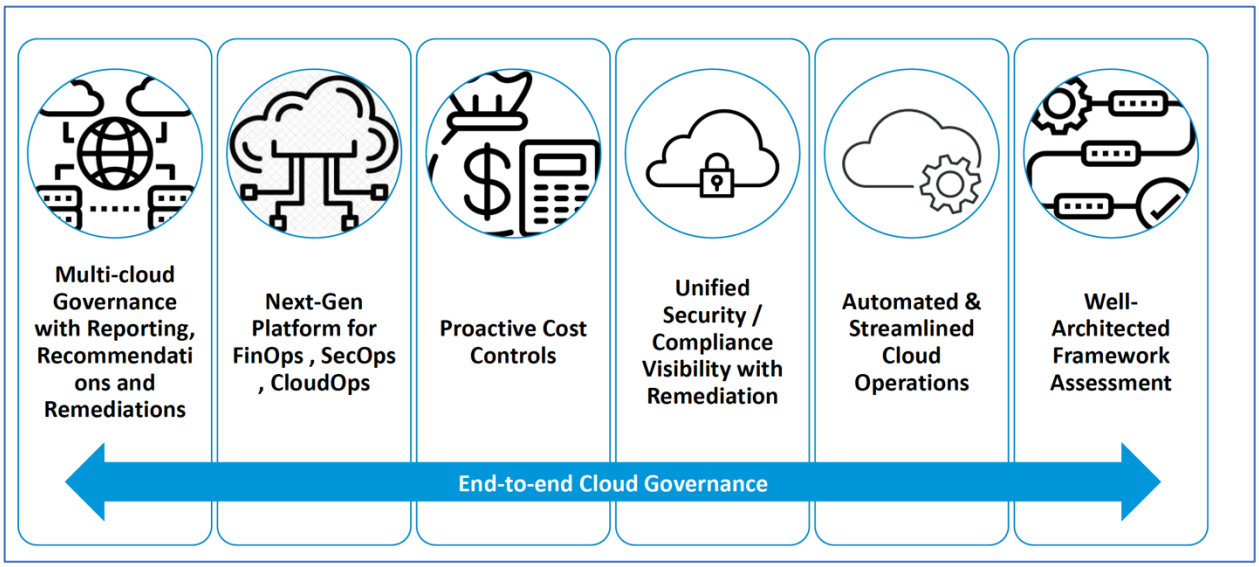
Tools Used:

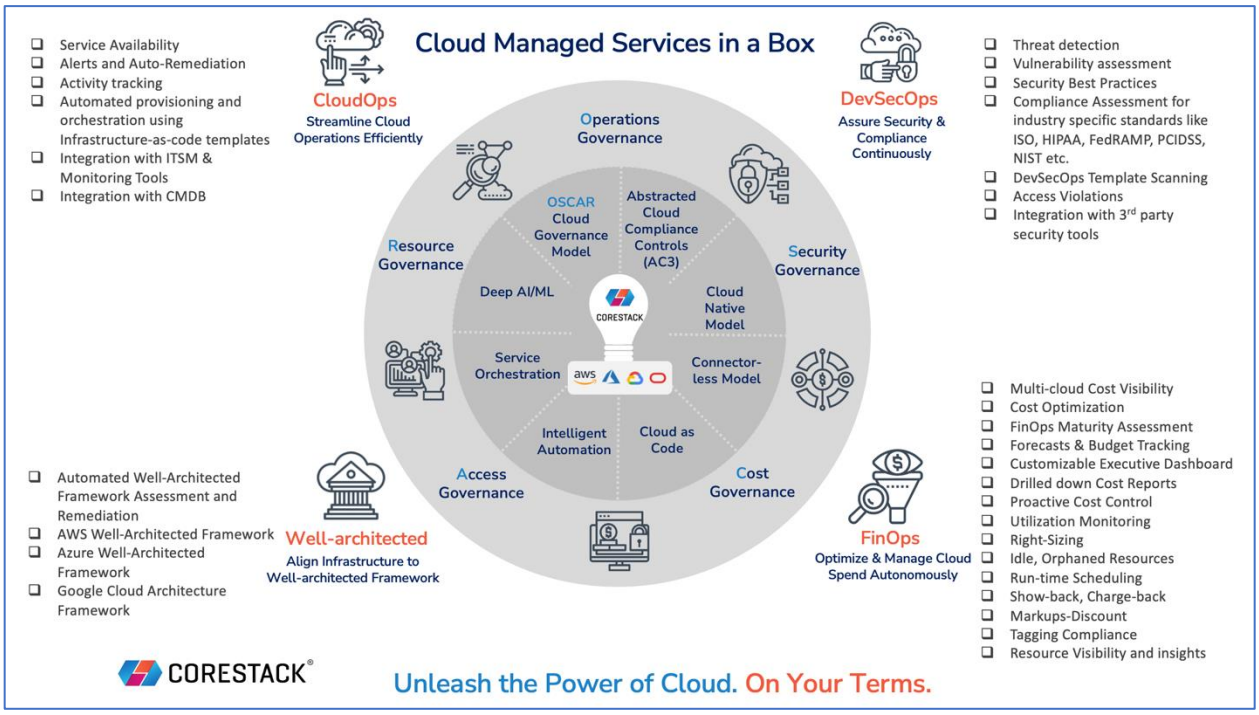
1. Azure Migration Assessment tool
2. Defender for Cloud
3. Cloudockit to generate the HLD and LLD
4. Microsoft Threat Management tool
5. VAPT tool if needed (after migration to check)
6. Corestack (FinOps, GRC tool for Cloud)
7. Terraform or ARM templates for IAC
8. Azure Devops / Azure Runbooks for CloudOps automation
9. Azure Well Architected Review tool
10. Azure Strategic Migration Assessment tool
11. Governance Benchmark tool
12. Go-Live Well architected Review tool

CORESTACK FOR FINOPS AND GRC:






Multi-cloud Governance with Reporting, Recommendations and Remediations
Next-Gen Platform for FinOps , SecOps , CloudOps
Proactive Cost Controls
Unified Security / Compliance Visibility with Remediation
Automated & Streamlined Cloud Operations
Well-Architected Framework Assessment
End-to-end Cloud Governance


Cloud Managed Services in a Box
Service Availability
Alerts and Auto-Remediation
Activity tracking
Automated provisioning and orchestration using Infrastructure-as-code templates
Integration with ITSM & Monitoring Tools
Integration with CMDB
CloudOps
Streamline Cloud Operations Efficiently
DevSecOps
Assure Security & Compliance Continuously
Threat detection
Vulnerability assessment
Security Best Practices
Compliance Assessment for industry specific standards like ISO, HIPAA, FedRAMP, PCIDSS, NIST etc.
DevSecOps Template Scanning
Access Violations
Integration with 3rd party security tools
Operations Governance
OSCAR Cloud Governance Model
Abstracted Cloud Compliance Controls (AC3)
Resource Governance
Security Governance
Deep AI/ML
Cloud Native Model
CORESTACK
Service Orchestration
aws
Connector-less Model
Intelligent Automation
Cloud as Code
Access Governance
Cost Governance
Automated Well-Architected Framework Assessment and Remediation
AWS Well-Architected Framework
Azure Well-Architected Framework
Google Cloud Architecture Framework
Well-architected
Align Infrastructure to Well-architected Framework
FinOps
Optimize & Manage Cloud Spend Autonomously
Multi-cloud Cost Visibility
Cost Optimization
FinOps Maturity Assessment
Forecasts & Budget Tracking
Customizable Executive Dashboard
Drilled down Cost Reports
Proactive Cost Control
Utilization Monitoring
Right-Sizing
Idle, Orphaned Resources
Run-time Scheduling
Show-back, Charge-back
Markups-Discount
Tagging Compliance
Resource Visibility and insights
CORESTACK
Unleash the Power of Cloud. On Your Terms.