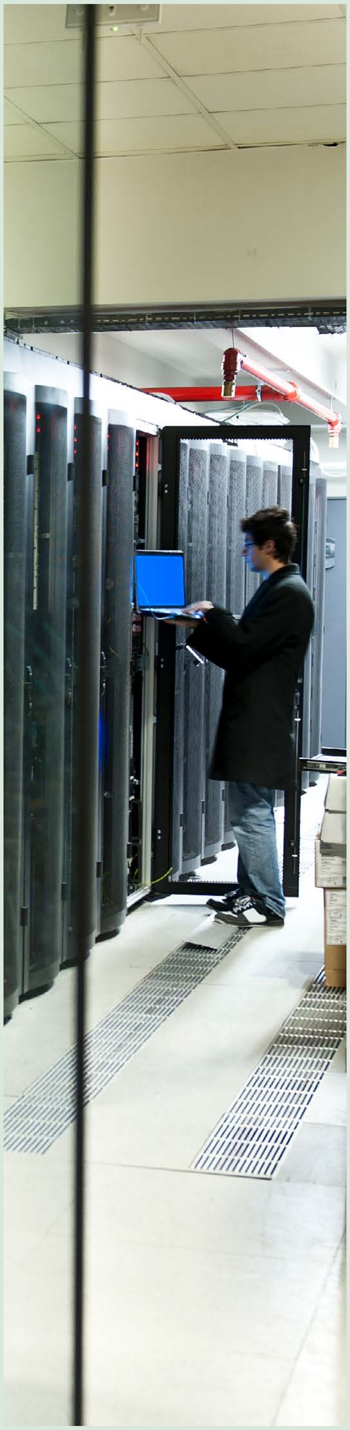
WHITE PAPER



CLOUD MIGRATION ASSESSMENT FRAMEWORK

Sahi, Ashish
Infosys Ltd.

Infosys®
Navigate your next

Abstract

Cloud is a popular choice for organizations seeking to become agile, reduce cost and ensure lean IT operations. However, with many new and established players in the market, most organizations are unaware of how to choose the right service provider and solution for their cloud migration journey. Without proper due diligence, cloud migration programs can prove expensive in the long term, limiting the ability of organizations to achieve real cost benefits, agility, scalability and portability.

This paper provides an assessment framework that can be used by organizations, product vendors, implementers, and systems integrators while evaluating cloud migration. By focusing on non-functional aspects such as security, sovereignty, resilience, storage, on-going maintenance, and cost of operations, this framework acts as a guide to ensure that cloud migration meets organizational requirements and supports future growth.

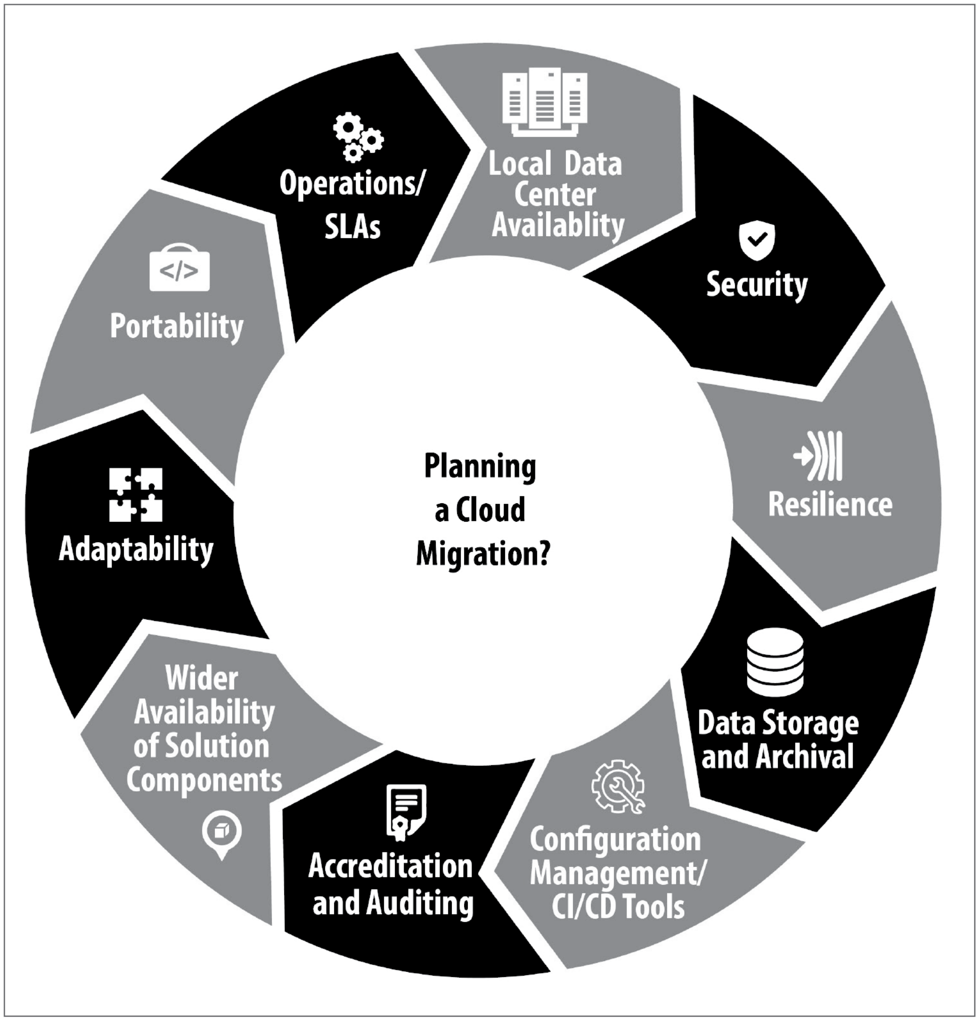
Introduction

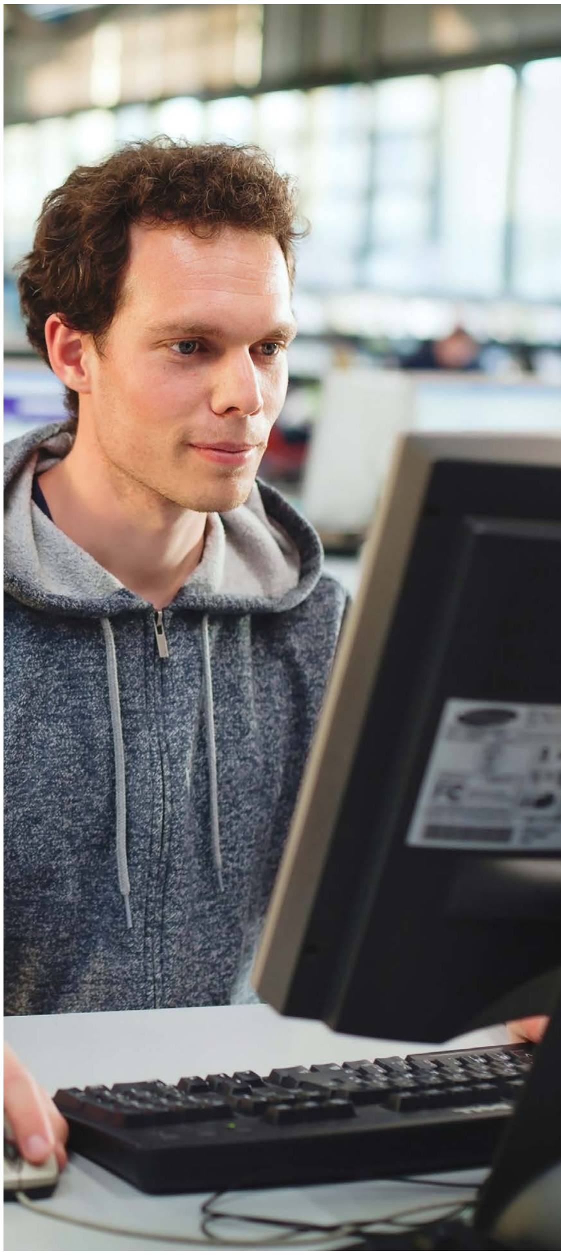
Over the past few years, there has been a significant increase in cloud implementations including greenfield implementations, cloud migrations and hybrid implementations. According to Gartner[1], the worldwide public cloud services market is expected to grow to US $383 billion in 2020 compared to US $209 billion in 2016. A majority of implementation programs over the last 5 years across industries and geographies have been cloud-based solutions. Further, these implementations have been supported by corresponding investments and offerings from product companies, systems integrators and client organizations.

The current breed of cloud service providers ranges from the oligopoly of global giants to a rapidly evolving cluster of local providers. However, despite the buzz around cloud migration, there is an alarming trend of inadequate due diligence, particularly for non-functional aspects. Low entry barriers, nominal initiation costs and sales to aspirational clients by cloud providers coupled with newly formed IT cloud strategies frequently result in cloud migration decisions being made without crucial due diligence.

Cloud migration assessment criteria

Organizations looking to implement cloud migration solutions must first evaluate how the planned migration will affect non-functional aspects within their enterprise. The following assessment framework provides some key criteria to be considered before planning a cloud migration journey.


Planning a Cloud Migration?
Local Data Center Availablity
Security
Resilience
Data Storage and Archival
Configuration Management/ CI/CD Tools
Accreditation and Auditing
Wider Availability of Solution Components
Adaptability
Portability
Operations/ SLAs



1. Local data center availability – Having a locally-available data center is an important consideration for organizations moving to cloud. Many countries have strong legal requirements around data sovereignty that prohibits the storage of customer data outside their physical boundaries. Thus, this is a critical assessment criterion that should be considered during the vendor selection process. Unfortunately, this aspect is often overlooked during the selection process, resulting in costly future consequences.

There are instances where the cloud provider prematurely commits to providing a local physical data center within a certain timeframe to skew the client's selection decision in their favor. It is strongly recommended that such dependencies be avoided and de-coupled right at the beginning. Companies must also assess readiness of a locally-available disaster recovery site where legal regulations do not allow data back-up to reside outside the country's boundary. This criterion is best applied at the inception (pre-discovery/ discovery) phase to avoid any regret spend down the line.

2. Security – Typically, cloud solutions introduce additional risk to a company's IT landscape and operations. In many instances, there is limited control over network and connectivity for externally-managed data centers is normally possible only over the Internet. While application programming interfaces (APIs) provide a quick and flexible way for integration, these often lack the right level of authorization. Thus, cloud vendors may have serious vulnerabilities in their products that often do not meet the client organization's security architecture and operations requirements.

Further, there may be different levels of security controls and gaps for software-as-a-service (SaaS), infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) offerings from the same cloud vendor. Such gaps need to be identified at the beginning and assessed for fitment accordingly as there is a high chance of

delayed platform-level patching. The lack of security architecture/operations review can result in major operational issues. In fact, there are several instances where solution components were immediately changed after the build cycle and the first review with security architecture. The reasons for this may vary; it could be due to lack of encryption during storage and transmission, lack of network control for SaaS offerings, lack of multi-factor authentication, publicly exposed repositories, inability to connect to a remote database, inability to connect over the Internet, etc. In some worst-case scenarios, some implementations were shelved because no one – not even the CxOs – could bypass the security risk.

Some client organizations may expect their cloud providers to enhance their security operations and associated NFRs. This is true for all organizations where IT architecture and security is not mature. Here, switching to a well-established cloud service provider could be a good risk mitigation strategy. In fact, large cloud service providers are making material investments2 in cloud security solutions to enhance the security profile of their services.

3. Resilience – Normally, most cloud service providers aggressively market their commitment to resilience. However, the recent Amazon Web Services (AWS) outage3 in February 2017 is a reminder that even the best can fail, making outages a key concern. The irony is that the AWS Service Health Dashboard, which should have reported the outage spread and recovery timeframes, was also affected. The lesson here is that business continuity should not be compromised for cheaper cloud platforms/solutions that do not offer full coverage. One may argue that even captive on-premises data centers are prone to outages/incidents. Nevertheless, organizations should make sure of their cloud vendors' resilience before transitioning operations.

Cloud service providers should be assessed for resilience based on high platform availability, proven procedures and ability to recover, validated response times for recovery, and the promise of continuity in case of an unforeseen event. In fact, this could even be the criteria used to shortlist cloud vendors. While paper-based assessments can be used during inception phase/s, it is important to validate all resilience measures during operational tests. Even a simple backup/restore task could involve significant effort in terms of planning, actual execution and acceptance to be ready for operations. Finally, organizations can also consider variable resiliency for less critical applications in cases where there is significant cost advantage and the function/data is not business-critical.

4. Data storage and archival – The global market for the cloud storage industry4 was valued at US $21 billion in 2015 and is estimated to grow at a CAGR of 24.8% to reach US $97 billion by 2022. By 2020, the total globally installed data storage capacity5 in cloud data centers will account for 88% share of total DC storage capacity compared to 64.9% in 2015.

Data, no matter how critical, needs to have a finite storage timeframe in conjunction with an active archival policy. This policy should be listed in the organization's data strategy and must be refined for cloud migration. It is important for organizations to define their data storage and associated capacity requirements upfront to ensure the right sizing and storage options on cloud. For an immediate cloud migration, clients must evaluate equivalence (existing capacity) as well as the extrapolated storage requirement for the first few years of operations (projected capacity).

Most cloud vendors have their own governance limits. Therefore, a good practice is to define what and when to archive. Organizations should look at permanently purging data that is not functionally or legally required. Cloud storage can be expensive and one cannot assume that it will be abundantly available. Thus, before implementing the platform, organizations must establish an archival strategy where archival costs on cloud versus on-premises are compared to ensure the right platform choice.

5. Configuration management, continuous improvement and continuous delivery tools – Cloud solutions are often associated with agile ways of working, which means that these solutions must support continuous delivery and continuous deployment with preferred tools. The chosen cloud platform must also be compatible with and support existing/targeted automation tools without compromise. While this may seem like a basic criterion, it is often overlooked by organizations.

It is also important to adopt configuration/repository management using tools chosen by the client organization. Often, organizations face issues such as public-facing repositories that are unacceptable from a security and integrity viewpoint, lack of a single and compatible configuration management tool for both cloud-based and on-premises applications for hybrid implementations, limited system access control for tools, etc.

Sometimes, organizations simply choose cloud components that are limited to basic application installation and set-up and allow developers to use local or on-premises repositories without defining any configuration management tool/process on cloud. Such situations must be avoided. While getting started with cloud may be relatively easy, it is important to pay attention to basic hygiene factors.

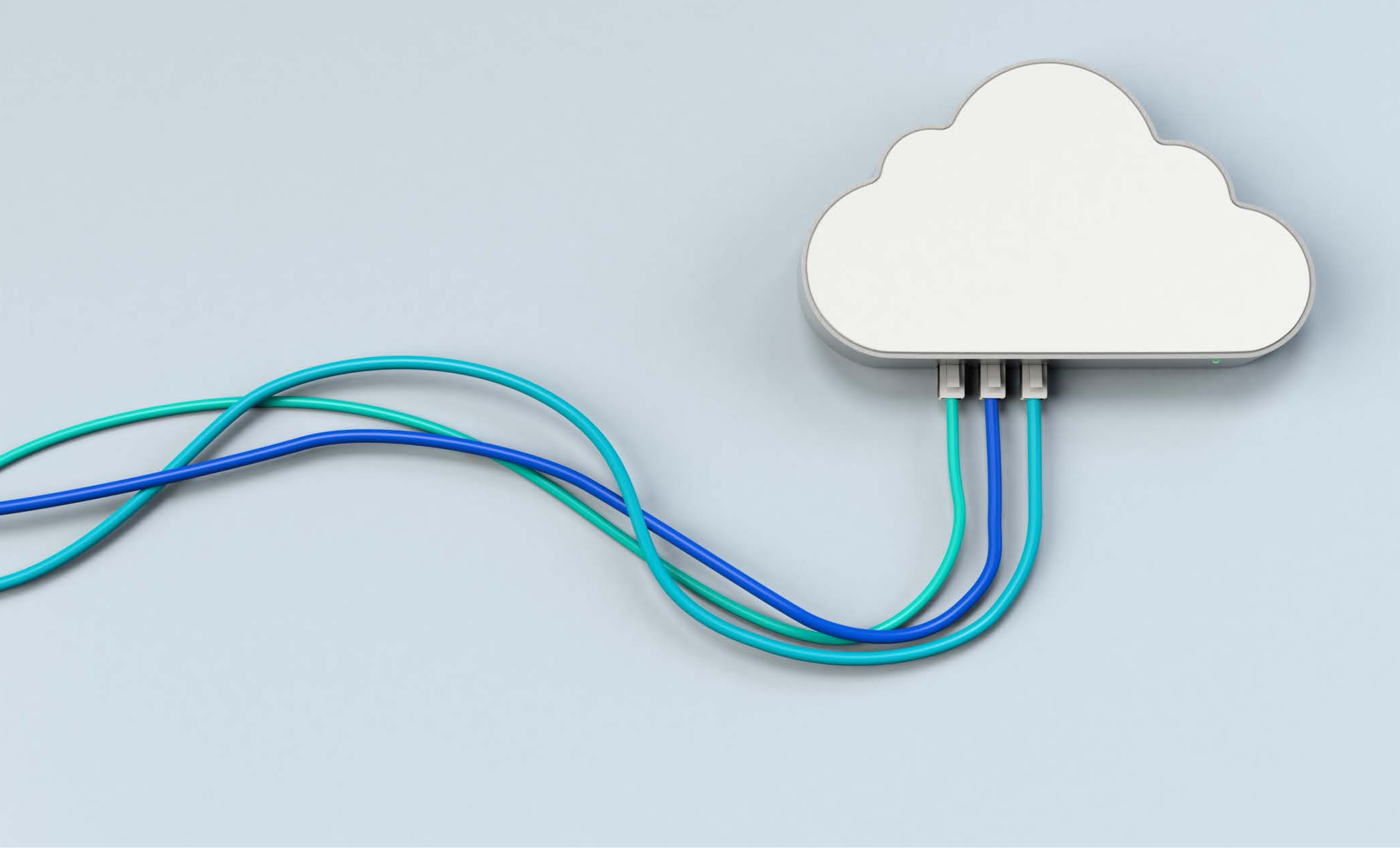
6. Accreditation and auditing – The rapid adoption of cloud services means that providers are flooding the marketplace. This makes it imperative for organizations to ensure that their chosen service provider has the right credentials and authorization and is committed to providing a minimum standard of service for managing organizational systems/data. For instance, when hosting personally identifiable information (PII) on cloud, organizations should check whether the cloud service provider is ISO/IEC 27018-certified or not. ISO/IEC 27001/27002 certification ensures a minimum level of security control as well as an information security management system. Similarly, cloud service providers should also be receptive and encourage the auditing of their security, network and other operations. Organizations and independent cloud auditors should be able to audit and review the complete setup as

part of the standard operating procedure. Such trust and transparency is vital to encourage organizations to move towards cloud.

7. Wider availability of solution components – The current cloud service provider mix is quite diverse. Most organizations tend to rely on a few large-scale cloud service providers who offer global services rather than the newer and small/medium-sized indigenous cloud service providers who are mostly confined to a particular geography or region. Limited reach and scale impacts the products/services mix offered by cloud service providers, particularly the local ones. Organizations must always look for a wide and open range of solution component offerings at the lowest possible prices. When it comes to implementation, organizations should not compromise the targeted architecture because a particular application technology, operating system or database cannot be hosted or contractually supported by a cloud service provider. Ideally, irrespective of size and scale, all cloud service providers must commit to supporting any client-specific technology requirements.

This expectation must be set across all product and service providers. While there are many companies that have transitioned to cloud, others have not. Therefore, it is important to build an extensible model that can also support interim technology requirements to help organizations migrate to cloud. Wider and easy availability of solution components is extremely vital to maintain and extend IT operations.

8. Adaptability – Cloud service providers should not be rigid and dictate their operating framework to client organizations. While best-practices for hosting and operating solutions are appreciated, cloud service providers should also be receptive to client-specific requirements. For instance, clients may want a separate dedicated tenancy with greater security controls so they can operate as a pseudo-private cloud. Cloud service providers must be able to support this. There could also be additional upliftment requirements such as enabling security patches or a particular technology, converting IaaS to PaaS or SaaS and vice-versa, onboarding a new product vendor, etc. All such requirements should be accepted and assessed for upliftment



to facilitate migration to cloud. In the case of hybrid implementations, a higher number of exceptions may be required and this is extremely critical to support cloud migrations.

9. Portability – Client organizations should be able to port out, migrate or switch service providers when needed. Low exit barriers should complement low entry barriers for cloud services and solutions. Further, the solutions developed on cloud should not be strictly coupled with a particular cloud service provider. In a recent cloud migration project, the Infosys team struggled to port out of a particular reporting application simply because the underlying data warehouse technology was specific (proprietary) to the existing service provider. This outcome could have been avoided by selecting a widely-available data warehouse technology at the beginning.

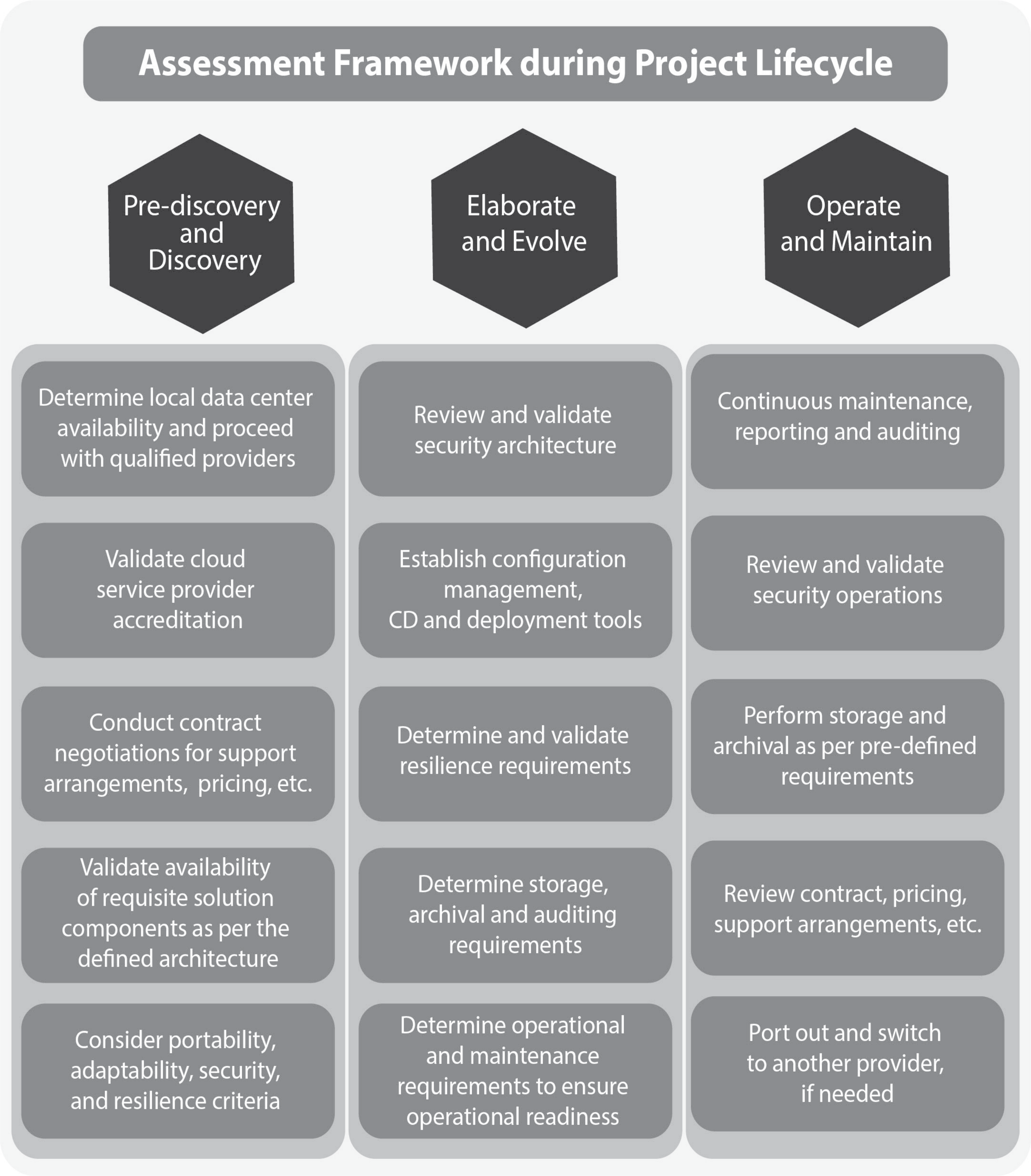
In some cases, a client organization may want to switch providers for better pricing and cost savings. While porting out solutions/applications may be uncommon in the industry, it pays to have this capability and option available. Ultimately, cloud migrations should liberate us from the traditional and hard dependencies on support/platform providers.

10. Operations/SLAs – Migrating to cloud should not compromise existing operational and maintenance SLAs for any client organization. Thus, the assessment criteria should clearly identify any potential deficiencies or constraints that could potentially hinder the client organizations to realize their improvement targets. It is important to note that the support arrangement and SLAs can vary considerably among SaaS, IaaS and PaaS offerings. Hence, organizations may want to independently measure the performance of cloud services and associated SLAs over and above the normal service dashboards rendered by cloud providers. Independent external service dashboards6 can be used to determine SLAs in the event of any dispute. It is also recommended to establish an RACI during contract negotiations to understand the components being supported by cloud service providers.

Typically, platform-level services (PaaS) and SaaS offerings receive moderate coverage. However, coverage for other services (IaaS) is often compromised. The difficulty lies in determining whether the cloud service provider or the application team is responsible for items like application back-up and restore, database back-up and restore, etc. Further, does this situation change for SaaS, IaaS or PaaS offerings? This is where due diligence becomes important. Cloud service providers must also commit to providing operational status reports weekly/monthly (over and above the standard availability dashboards/metrics) as defined by the client's operational requirements. There should also be a predictable charge model for ongoing services, onboarding additional solution components and any capacity extensions to enable the client organization to better plan their operational expenditure. Operational payouts to cloud service providers can be made outcome-oriented by linking cost to actual services realized.

Cloud migration assessment framework

The following diagram and table outline the recommended assessments to be conducted during the cloud migration lifecycle across pre-discovery, discovery, elaboration, and operations phases.



Assessment Framework during Project Lifecycle

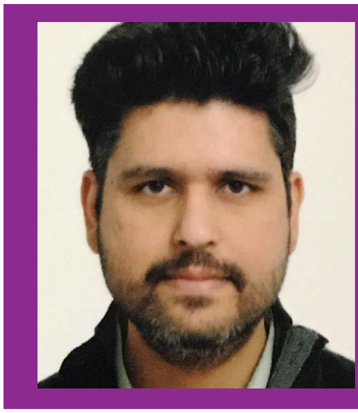
Pre-discovery and Discovery	Elaborate and Evolve	Operate and Maintain
Determine local data center availability and proceed with qualified providers	Review and validate security architecture	Continuous maintenance, reporting and auditing
Validate cloud service provider accreditation	Establish configuration management, CD and deployment tools	Review and validate security operations
Conduct contract negotiations for support arrangements, pricing, etc.	Determine and validate resilience requirements	Perform storage and archival as per pre-defined requirements
Validate availability of requisite solution components as per the defined architecture	Determine storage, archival and auditing requirements	Review contract, pricing, support arrangements, etc.
Consider portability, adaptability, security, and resilience criteria	Determine operational and maintenance requirements to ensure operational readiness	Port out and switch to another provider, if needed

	Pre-Discovery/Discovery	Elaboration/Evolve	Operate/Maintain
Phase Description	This is the inception phase and includes: ✓ Idea assessment ✓ Business case validation ✓ Business requirements consolidation ✓ Cloud product/service provider assessment and selection ✓ Commitment to application/product development	This is the implementation phase and includes: ✓ Solution/design detailing ✓ Requirements elaboration ✓ Build ✓ Testing including system, application, integration, performance, and operational tests ✓ Production deployment ✓ Commitment to operate	This is the post-deployment operations and maintenance phase and includes: ✓ Application/product workability in production ✓ Ongoing support and operations management ✓ SLA adherence ✓ Reporting and auditing ✓ Continuous improvements and deployments
Local Availability	✓ Validate data sovereignty requirements. Do not proceed if these are non-compliant	✓ Closely monitor and track any local data centre development, if such was promised during the inception phase	✓ Deploy the data center in compliance with data sovereignty requirements
Security	✓ Ensure that the cloud product and cloud service provider are committed to meeting the security requirements	✓ Review and validate security architecture. Do not begin implementation based on assumption of security services ✓ Encourage early review with operations on security compliance	✓ Ensure security operations are compliant before deployment ✓ Conduct ongoing review, upliftment, patching, etc., for better security control
Resilience	✓ This is a key criteria for selecting the cloud service vendor ✓ Ensure support for organization's business continuity	✓ Define and agree on variable resilience requirements depending upon business criticality ✓ Review and agree to terms with operations	✓ Ensure adherence to promised resilience requirements ✓ Ensure preparedness for unplanned events and outages
Data Storage and Archival	✓ Assess the organization's data storage capacity for the first few years of operations	✓ Define data strategy, i.e., what to store and when to archive	✓ Ensure data storage is in line with data strategy ✓ Provide support and auto-trigger archival
Configuration Management/CD Tools	✓ Articulate requirements for continuous integration/delivery	✓ Immediately establish CI/CD framework to support and optimize build and deployment efforts ✓ Define release cadence	✓ Support continuous deployments in line with the defined release cadence
Accreditation and Auditing	✓ Conduct hygiene checks on cloud product/service provider accreditation ✓ Review the existing auditing supported by cloud provider	✓ Validate accreditation, i.e., is the existing PII or security accreditation sufficient? ✓ Determine any additional auditing requirements	✓ Ensure provider accreditation is maintained and additional certifications are met where needed ✓ Conduct continuous auditing and ensure a governance process is present to manage conflicts/gaps
Wider Availability of Solution Components	✓ Review cloud service provider offerings ✓ Validate availability and support of all requisite solution components	✓ Ensure implementation of the right solution components in line with the defined architecture	✓ Ensure ongoing operations, support and upgrade
Adaptability	✓ Define bespoke requirements as an assessment criteria and ensure cloud service provider commitment to deliver these	✓ Validate implementation of bespoke elements ✓ Agree on framework for extensions and changes	✓ Extend support for bespoke elements. This should to be included as part of the standard operations
Portability	✓ This is a key design principle: Prioritize generally-accepted and widely-available components to ensure low exit barriers	✓ Thoroughly review the selection and implementation of selected components during the build phase	✓ Ensure ongoing support and avoid custom components/frameworks that mandate strict coupling with the provider ✓ Port out when needed

Conclusion

Today, cloud migration is no longer just an IT strategy; it also represents the core of an organization's business strategy. Organizations contemplating the move to cloud need to be aware of the business problems they face and how cloud can solve these. While most players are able to understand and resolve initial migration challenges, the long-term implications of cloud migration are yet to be fully comprehended. This makes it critical to do a thorough due diligence when preparing for a cloud migration.

The framework presented above will help organizations evaluate non-functional aspects before migrating to cloud. These aspects include local data center availability, security, resilience, data storage and archival, configuration management, continuous improvement and continuous delivery tools, accreditation and auditing, wide availability of solution components, adaptability, portability, and SLAs. While this framework is not exhaustive, additional criteria may be appended to this framework during assessment.



About the Author

Ashish Sahi is a Lead Consultant in Infosys having more than 11 years of experience in process and domain consulting, business analysis, solution designing, IT project and delivery management. He is part of CX Oracle practise involved in delivering solutions across CRM, BSS, Oracle, Cloud, Data, Digital Technologies & Integration.

References

1. http://www.gartner.com/newsroom/id/3616417
2. https://go.forrester.com/blogs/17-06-08-cloud_security_spending_will_grow_to_35_billion_by_2021/
3. https://aws.amazon.com/message/41926/
4. https://www.alliedmarketresearch.com/cloud-storage-market
5. https://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.pdf
6. https://cloudharmony.com/status

For more information, contact askus@infosys.com

Infosys®
Navigate your next

Infosys.com | NYSE: INFY

Stay Connected SlideShare