**Cloud Migration: Fundamentals and Challenges**

Arthur H. Neumann

Carnegie Mellon University  
95-705 – Telecommunications Management  
Dr. Sakir Yucel

July 30, 2022



Executive Summary

Managing information technology (IT) services can be a costly endeavor. For small businesses to multi-national corporations, funding and managing IT operations can often divert critical organizational resources away from the primary business focus. Balancing IT requirements with business needs remains a significant challenge for many organizations. Fortunately, as technology has improved, cloud services have become a viable alternative to in-house IT systems, allowing organizations to purchase customized environments tailored to their needs. Furthermore, cloud environments have enabled organizations to expand and contract rapidly to support business requirements. With the COVID-19 pandemic and rising inflation, many businesses are looking to save in any way they can, and substantial investments are being made in the cloud computing market to reduce the costs of hosting IT infrastructure internally.

Organizations looking to take advantage of cloud services must first understand what cloud computing is and what it is not. This paper provides a high-level overview of cloud terminology and functionality, discusses how to plan a cloud migration properly, outlines how to identify the requirements for cloud migration and select an architecture based upon organizational business needs, and identifies common migration activities, challenges and mitigations. While this paper outlines core requirements for designing a cloud migration, it does not provide specific cloud technology recommendations. Instead, it aims to provide a management-level understanding of the effort associated with cloud migration projects.

Before undertaking a cloud migration project, organizations must understand the available solutions and use a well-informed decision-making process to decide whether cloud-based IT services can help them achieve their business goals and reduce IT costs. Organizations electing to implement a cloud strategy must embark on a complex process of planning, designing, and implementing a cloud strategy. Before beginning a migration effort, organizations must understand the significant concerns and challenges of cloud implementations and ensure that sufficient resources are allocated to successfully address each challenge and ensure the overall success of the migration process.

Table of Contents

[Executive Summary 2](#_Toc110602297)

[Cloud Migration: Fundamentals and Challenges 4](#_Toc110602298)

[Cloud Fundamentals and Services 4](#_Toc110602299)

[Cloud Fundamentals 4](#_Toc110602300)

[Cloud Services 5](#_Toc110602301)

[Cloud Migration Process 5](#_Toc110602302)

[Planning 5](#_Toc110602303)

[Functionality Review 5](#_Toc110602304)

[Environment Assessment 6](#_Toc110602305)

[Strategy Selection 7](#_Toc110602306)

[Migration 12](#_Toc110602307)

[Service Disruptions 12](#_Toc110602308)

[Cost 12](#_Toc110602309)

[Time 12](#_Toc110602310)

[Cutover 13](#_Toc110602311)

[Cloud Migration Challenges 13](#_Toc110602312)

[Security 14](#_Toc110602313)

[Vendor Lock 14](#_Toc110602314)

[Legacy Systems 15](#_Toc110602315)

[Cost Management 15](#_Toc110602316)

[Findings and Recommendations 15](#_Toc110602317)

[Findings 16](#_Toc110602318)

[Recommendations 16](#_Toc110602319)

[References 18](#_Toc110602320)

Cloud Migration: Fundamentals and Challenges

Information Technology (IT) has enabled organizations to look for new and innovative ways to integrate technology into their business services, operations, and processes to enhance their ability to achieve organizational goals and improve profitability and efficiency. Today’s most successful organizations rely heavily on IT resources to provide new capabilities and opportunities for growth. It is not uncommon for many businesses to leverage some form of data analytics or Artificial Intelligence and Machine Learning (AI/ML) to identify business trends or make business predictions. Increased demand for higher-performing IT resources and substantial costs of managing and supporting on-premises data centers have driven many organizations to seek alternative methods of obtaining cost-effective IT resources without the administrative overhead of managing their own data center. As a result, many organizations have looked to Cloud Solutions Providers (CSPs) to meet their IT needs while minimizing costs. As evidence of this move to the cloud, technological research and consulting firm Gartner has forecasted worldwide spending on cloud infrastructure to grow by 20.4% in 2022 to USD 494.65 Billion (Rimol, 2022). While there are significant opportunities for cost savings and growth by leveraging cloud solutions, organizations seeking to capitalize on cloud infrastructure need to ensure they understand available cloud services, architectures, core migration activities, and potential challenges. A firm understanding of cloud solutions is key to a successful migration. Due diligence in requirements definition and planning can significantly improve strategy choices and the overall success of cloud design and workload migration.

# Cloud Fundamentals and Services

Cloud computing started alongside the publicly available internet and was first used to describe the technology between end users and ISPs. However, it was not until the late 1990s and early 2000s that technological advances enabled services similar to those we are familiar with now, such as Salesforce and AWS. Today’s cloud computing has a unique vocabulary and functionality set just like many other IT areas. Understanding core concepts of cloud services is fundamental to a successful migration.

## Cloud Fundamentals

Cloud services offered by a CSP come in many different forms. Most customers, or tenants, of a CSP, access their cloud services and resources using the internet or Wide Area Network (WAN) connectivity. The main types of cloud computing are grouped into three categories, public, private, and hybrid cloud. In a public cloud, organizations connect to cloud resources that may be co-located or shared with other organizations via the internet. In a private cloud, the organization connects to a cloud environment explicitly dedicated to one organization—finally, organizations using a hybrid cloud mix both public and private cloud environments.

## Cloud Services

Standard services offered by CSPs include Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS). In an IaaS environment, the customer leases hardware and receives access and connectivity to IT hardware, including servers, networking equipment, and storage systems. In an IaaS environment, the customer is responsible for most of the system functionality and is free to configure and manage the devices as they see fit. In a PaaS environment, customers receive access to a pre-provisioned service upon which they can install applications and services. PaaS systems managed by the CSP enable customers to reduce the resources required to maintain the environment. In the SaaS model, the CSP manages and maintains all underlying functionality and provides access only to specific software applications affording businesses with access to vendor-made applications supporting business functions.

# Cloud Migration Process

## Planning

Understanding organizational IT requirements and prior planning is key to minimizing the work required to implement a cloud solution. Ensuring cloud environment design considers overall business strategy and needs, IT services supporting critical business processes, services, and activities before choosing a service or designing a cloud architecture maximizes an organization’s return on investment (ROI). Furthermore, proper planning and analysis ensure cloud systems adequately support the demand and growth of each IT service and reduce the likelihood of gaps in functionality or performance, double work, and unforeseen expenditures.

### Functionality Review

The first step of defining the requirements of a cloud environment requires organizations to identify the system functionality and capability required. For example, the needs of an organization developing applications will differ significantly from a business providing legal services. Before selecting a cloud service, organizations must identify business functions, core processes, and activities and the core IT functions and services supporting each area. This information can be obtained by reviewing the overall business strategy and documentation such as a Business Impact Analysis (BIA) or Business Continuity Plan (BCP). Before moving forward with any cloud migration, it is critical to understand the IT services required to support the organization’s overall strategy and functions. This understanding will help determine a cloud project’s scope, timeline, and budget and set the foundation for identifying system-level requirements for each IT service.

### Environment Assessment

Following an initial assessment of the business's core functions, services, and activities, the next step is identifying the high-level requirements for IT services supporting the organization and the type of workloads using IT services. This information is critical for moving forward with cloud migration planning as it helps drive the business case, determines if the benefits of migration make sense from a time and resources standpoint, and aids in establishing the scope of services to be migrated to the cloud.

#### Business Requirements

Using the organization’s core functions, practices, and activities identified in the use case and functionality review, an analysis determining the types of work performed to support each area is required. Identifying the types of work being performed using IT services further drives IT service requirements and can be leveraged to determine goals for cloud infrastructure, including identifying core hardware and software functionality, performance, and capacity. Common types of work include application development, web hosting, data analysis, artificial intelligence, and administrative business operations. Every kind of work leveraging IT services has unique performance, capacity, availability, reliability, and compliance requirements that must be considered.

#### Workload Types

Once IT services and the types of work performed using IT systems are defined, the next objective is to determine system requirements is identifying high-level system specifications for each service, including hardware, software, connectivity, and security requirements. Practical analysis of system requirements should entail a review of any existing IT infrastructure and applications and consider the type of devices, i.e., servers, storage, and network connectivity, as well as any potential security configuration or compliance requirements. This review must also identify high availability, disaster recovery, redundancy, and continuity of operations requirements to identify configurations required to align technology requirements with required service functionality. A way to measure these requirements is by evaluating system and service requirements and establishing key performance indicators (KPIs) that provide quantifiable metrics for each service. Once each service has been mapped to high-level system requirements, a detailed review of the workloads performed on the system will identify the individual system requirements for each device supporting the IT service.

#### System Requirements

With a broad understanding of the high-level operational requirements, detailed system-level requirements can be defined for each IT Service, including system hardware, networking, and storage specifications to meet system performance and capacity requirements. When performing a specification analysis, the organization must review each system's functionality and application requirements for CPU, GPU, memory, network, storage, and operating system types. A method to achieve this is first to analyze the kind of work performed on each system, i.e., data processing, web services, or data storage, and then examine the requirements specifications for each application running on a device. These requirements can be mapped to the KPI requirements defined during the workload assessment. Once the exact system specifications are determined, the organization should perform a holistic review of the overall requirements, including a review of potential bottlenecks to system and service performance, and identify any additional necessary system requirements for operation. Using each IT system’s detailed requirements, the organization can forecast additional requirements to support future growth and expansion within the IT environment.

#### Growth and Expansion Requirements

Using the organization’s business strategy and identifying any potential business growth relying upon IT services, the organization must also ensure that IT service and system specifications consider additional demand that may result from business or service growth. An analysis of potential growth specifically must consider added system performance and capacity requirements to support the increased workload and forecast the timeframe in which new requirements will appear.

### Strategy Selection

Following a comprehensive evaluation of all functional requirements, a strategy for cloud migration can be developed. This strategy should be represented in a business case that outlines the migration's scope, integration methodology, identifies cloud technology selections, and establishes a timeline and budget for the migration.

#### Business Case

With all preliminary assessment activities completed, a business case for each service and application evaluated for potential cloud migration is developed using the current business strategy and service requirements along with identified system requirements. Ideally, each business case should evaluate organizational needs with service offerings from a CSP and identify the improvement of operational capability, cost reduction, and technology capabilities. The business case should provide decision-makers with a high-level overview of the benefits, potential drawbacks, and risks of migrating on-premises technology to the cloud.

#### Scope Definition

Each business case should clearly define the scope of the IT service or application being evaluated and ensure that all necessary support systems are considered in establishing the cloud environment. This consideration should include systems and services supporting common operations within an IT environment such as routing and switching connectivity, core services such as DNS, DHCP, and a security stack including firewalls, vulnerability, and endpoint protection where necessary. A well-defined scope can help prevent budget and timeline overruns associated with missed requirements and scope creep.

#### Methodology Selection

##### Cloud Type and Services

After determining all business and system requirements, a cloud implementation methodology can be selected. This methodology identifies the best-suited cloud type, i.e., public, private, or hybrid cloud, and the type of cloud services to be purchased, i.e., IaaS, PaaS, SaaS, or any combination of the three. This decision also must consider the approach that will be used to migrate services and systems to the cloud environment, i.e., a greenfield or brownfield approach. Using a greenfield approach, the organization designs and implements an entirely new environment with new technologies and architectures tailored to their current and future IT needs. Under a greenfield approach, organizations can refactor, revise, rebuild or replace technologies and devices using IaaS, PaaS, or SaaS to meet requirements. Organizations that use a brownfield approach by rehosting or lifting and shifting systems to the cloud typically choose IaaS cloud services to mimic their existing data center environment. If cloud services are chosen correctly, they allow organizations to capitalize on substantial reductions in data center facilities, system maintenance, and IT overhead. Reducing IT costs and overhead enables organizations to focus on their primary business objectives instead of running a full-scale IT operation internally.

##### Cloud Service Elements

As IT services are chosen for cloud migration, it is essential to consider the overall operations of the cloud environment in the following areas, cloud security and compliance, architecture and capabilities, manageability, service levels, support, and cost models (Threat Stack, 2022). Each additional service can dramatically impact the cost of implementation or maintenance and influence the architecture or service selection based on the organization’s needs and requirements.

Cloud security and compliance play a significant role for many organizations storing sensitive data, including Personally Identifiable Information (PII), Protected Health Information (PHI), Payment Card Information (PCI), business sensitive or confidential information, or information that falls under various federal, state, and local, government regulations. These regulations may apply within the organization’s country of origin and any foreign nations where it conducts business. Compliance may require co-locating data and not exporting or storing it outside specified national boundaries or specific system configurations and controls to ensure the data is adequately protected from disclosure. These security and compliance requirements can impact the overall cost of the solution and should be a primary consideration for every cloud service selection.

Available architectures and capabilities may vary significantly from CSP to CSP, and additional perks for choosing a specific CSP to host a particular application or service may exist. There is also the potential for vendor-specific functionality to only be available from a particular CSP, which is particularly true for SaaS cloud services. A holistic approach to CSP selection should be taken to ensure that solutions are designed considering each CSP's overall cost of services and capabilities. In some scenarios, it may make sense to utilize a best-in-class hybrid approach to obtain all necessary abilities at the best price. However, when leveraging multiple CSPs, special consideration should be given to identify and minimize potential bottlenecks and the cost associated with moving data from provider to provider.

Another cloud service element that must be considered is the overall management and manageability of the cloud environment. Control of the cloud environment includes the ownership split for performing standard administrative functions for the environment. Organizations must consider the overall level of involvement they intend to perform and decide what functionality they want the cloud service provider to be responsible for, ensuring that all required management functions are covered. Management activities may include configuring and maintaining network connectivity, installing, configuring, updating, and maintaining operating systems, and vulnerability remediation. Additionally, customers may consider purchasing a pre-configured environment or using CSP or third-party consulting services to create, manage, or support an environment. If third-party or consulting services are leveraged for any portion of the project, careful attention should be paid to service level agreements (SLAs) and contractual agreements. Organizations using CSP or third-party services should also carefully consider and align ownership of cloud environment management with operational and cost requirements.

With IT systems no longer residing in an environment owned and managed internally, organizations must review and accept CSP and IT service provider SLAs to ensure that IT systems remain available, responsive, and provide adequate capacity and support. When choosing an SLA for a cloud service environment, organizations must consider that as SLA requirements get more demanding and less flexible, that cost will become a significant factor. Another area in which SLAs become important is their impact on organizational compliance with security frameworks, controls, and privacy regulations. SLAs may also define where data can and cannot be stored. As such, the organization must ensure that SLAs meet compliance requirements and do not introduce the possibility of legal litigation or unacceptable business operations disruption.

While an SLA may define many aspects of support, ensuring adequate support for the environment once established is paramount. Since cloud environments operate in another organization’s data center, inevitably, some form of support will be required. Everyday support activities may include adding or modifying services, troubleshooting connectivity or hardware failures, or validating compliance configurations of the service provider. Identifying necessary support services from the cloud service provider will improve responses to outages and minimize system downtime. There are different strategies for obtaining support, including live technical support via phone or chat, email, or online ticketing, and dedicated support staff hours, each with its own cost and availability models. Selecting the minimum model to meet service availability requirements can be used to maximize uptime while minimizing costs.

Each element of the cloud strategy plays a significant role in determining the overall cost of the cloud solution; however, a few more considerations may impact the price. The first is the size of the CSP being used. Larger CSPs with an extensive portfolio and massive data centers can afford to pass on savings opportunities for each cloud component leveraging economies of scale; however, they may charge more for their unique offerings and management services. Smaller, less established CSPs might offer lower costs using new cost models or innovative new services to incentivize customers to choose their platform. Finally, CSPs may offer discounts for customers bundling services, purchasing more services, and agreeing to reserve specific resources for extended periods. Cloud pricing models can be a bit convoluted, but the main types of pricing typically fall into a few distinct categories, pay-as-you-go, reserved, or volume. Each CSP service cost model should be carefully evaluated to determine the total cost of ownership (TCO) for hosting each IT service in the cloud.

#### Timeline

Another component of the migration strategy and business case, as well as an essential contribution to budgetary consideration, is the timeline for the migration. The migration’s timeline must be aligned with business operations requirements and minimize any potential service outages so as not to disrupt business functions. The timeline must reasonably consider the time necessary to successfully build and prepare a stable cloud infrastructure or environment, migrate system functionality, test operational capabilities, and transition services to the cloud environment following successful testing.

#### Budget

With a defined scope, timeline, and cloud strategy, the organization can now accurately estimate the overall cost of the migration and use realistic estimates of cloud service fees to identify the TCO for cloud services required to support each application. The TCO should incorporate the cost of all cloud services necessary to meet business needs, growth and expansion costs, and any additional potential costs, including application licensing, other required services, and IT administration. Furthermore, the budget should identify potential areas where the risk of cost overrun is a concern and establish mitigating controls to prevent the migration or ongoing services from exceeding estimated costs.

## Migration

After completing migration planning activities and obtaining an approved migration strategy and budget, the next phase is executing the cloud migration plan and migrating IT services and systems to the cloud. During this phase, three primary considerations are required for a successful migration, minimizing service disruptions, costs, and time. Using project management fundamentals, organizations can manage the migration project and work with business units, IT staff, and the CSP to minimize the impact of potential issues arising from migration activities. Depending upon the strategy selected, the overall migration itself may look very different for each service or system; however, the overarching goals and management tools for the migration will remain the same, improve business capabilities and technology, save resources, and reduce cost.

### Service Disruptions

There is always a potential for service disruption and outages during any IT evolution. Cloud migrations can be very complex, and cloud hosting environments can differ significantly from an on-premise environment. Most migrations will require integrating multiple technologies and consistent communication and feedback from various organizational stakeholders throughout the migration to ensure solutions are implemented and function correctly.

### Cost

Even though organizations should conduct a thorough cost assessment during the planning phase of cloud migration, there is always the potential for unforeseen challenges that can dramatically impact the overall cost of the migration. Throughout the migration, IT staff conducting the technical portion of the migration must be in direct communication with the business units utilizing the services. Using a project management approach to migration execution will allow organizations to identify roadblocks and additional costs and provide time for strategies to be updated in alignment with newly discovered migration requirements. Lastly, an organization needs to know when to stop a project due to excessive cost overruns. Setting clear financial guardrails for cloud migration will prevent organizations from wasting excessive resources attempting to finish an already failing project.

### Time

With requirements such as initial provisioning, data migration, and testing, there is always a potential for delays in migration activities. While extensive planning can offset the likelihood of project delays, there is always the potential that known unknowns can interfere with the migration timeline. The key to dealing with migration delays is ensuring active communication with key stakeholders and readjusting the timeline as necessary. Another critical factor is ensuring that the timetable for the migration allocates sufficient time for each activity. A common pitfall to cloud migrations is rushing through each activity to save on costs or get operations up and running as quickly as possible. By allocating adequate time for each activity, critical applications can be migrated safely after environment functionality has been thoroughly tested. Every migration should have clear guidelines for discontinuing a project due to a failure to meet project goals within a reasonable timeframe and budget. Like cost management, knowing when to stop project work and return to the planning phase to address significant concerns can save organizations considerable time and resources and prevent disruptions to business services.

## Cutover

The most sensitive time for any cloud migration is during the cutover. In the cutover phase, service requests are transferred from on-premise systems to cloud systems. Without proper testing and planning, this phase can cause a substantial disruption to organizational functions resulting in financial or reputation losses. Careful consideration must be given to each cutover activity and system. While there are many points of failure during cutover, three essential items must be monitored, system cutover order, data synchronization, and system performance. To provide all necessary services required for migrating applications, organizations must ensure systems are cut over in a specific order to ensure that prerequisites for each application are present in the cloud environment before moving forward. Most applications have specific data requirements, and for systems depending on services such as databases, data synchronization management is crucial to minimize the time required for the final synchronization and the amount of time the system cannot access data required to function. Finally, organizations must closely monitor each system as they are cutover to validate system stability and functionality post-cutover before continuing migration activities.

# Cloud Migration Challenges

While cloud environments can be designed to be very similar to on-premise environments, there are distinct features that make them behave differently from on-premises data centers. Due to these differences, substantial challenges need to be considered throughout a cloud migration. Luckily, with every challenge, there are ways for organizations to mitigate risk, reduce the impact of differences, and capitalize on the very differences that make cloud environments unique. While this paper does not describe every potential issue, it does identify common challenges experienced by organizations moving IT services to the cloud.

## Security

Security is one of the most significant potential challenges organizations will face migrating services to the cloud. Organizations leveraging CSP services through the public cloud must be aware of the implications associated with co-tenancy and ensure that the cloud services they have chosen are aligned with compliance and security requirements. Organizations that have not exercised due diligence and care in protecting sensitive data such as PII, PHI, PCI data, or information covered by other legal requirements may face steep legal penalties and significant impacts to their business reputation. The shared nature of public cloud services requires unique controls and security hardening to ensure that all data is adequately protected. Furthermore, specific security or compliance requirements may dictate the areas in which data can be stored. Physical storage location requirements necessitate organizations using the cloud to establish specific SLAs to ensure cloud-hosted data does not fall outside acceptable boundaries. Examples of territorial storage requirements include sensitive governmental data identified by the United States Department of Defense in DFARS 239.7602-2 or the private data of European Union (EU) citizens as dictated by the EU’s General Data Protection Regulation (GDPR) (European Data Protection Board, 2019; GSA, 2022). Failing to consider security and compliance can cause additional expenditures or even force an organization to move its IT services back to an internal data center.

## Vendor Lock

Another major challenge organizations deciding to utilize CSP services must be conscious of is vendor lock. While organizations using lift-and-shift migrations on IaaS may not have to worry about this challenge as much, organizations designing their applications for specific PaaS or SaaS systems must be aware that these systems may differ significantly from other CSP offerings. Unique CSP services can make migration to another CSP or back to an on-premise environment challenging and expensive. Minimizing unique service offerings or choosing widely supported services can save organizations in the long run if CSPs increase prices or discontinue specific services over time. Organizations must also consider the cost of migrating their data out of the cloud, as the cost of extracting data from cloud storage environments can be prohibitive, particularly for large quantities of data. These additional costs can force organizations to stay with a CSP and reduce their ability to receive preferential pricing from competing CSPs.

## Legacy Systems

Legacy systems pose a significant challenge for cloud migrations. Many legacy systems require unique operating configurations that may not be available for purchase in the cloud. There are only a few migration options for many of these systems. These options include replacing legacy systems using modern service offerings, migrating some functionality and augmenting with cloud service offerings well-suited for cloud environments, migrating the entire application to the cloud using virtualization of the legacy systems, and re-designing the system and migrating the data into a cloud-specific climate. Legacy systems are exceptionally challenging for cloud deployments because they often lack adequate support or have unique and specific system requirements.

## Cost Management

Organizations incapable of sustaining a cloud environment due to a lack of funding may suffer drastic consequences, particularly if the cloud environment is hosting critical business systems. Managing cloud migration and environment maintenance costs post-migration is another major challenge for organizations leveraging cloud services. Improper cost assessments can quickly result in catastrophic failure. Businesses must pay careful attention when estimating cloud costs and need to ensure that all areas are considered before moving IT services into the cloud. Complicated pricing models for accessing data in cloud storage can quickly lead to unforeseen additional costs. Other expenses associated with growth and data extraction from the cloud also cannot be overlooked.

# Findings and Recommendations

Like many other IT projects, cloud migrations are complex and require substantial planning to execute successfully. Despite detailed planning, cloud migrations are as prone to failure as any other IT project due to their complexity. Treating cloud migrations as a traditional IT project and ensuring that thorough planning is performed ahead of time can help reduce the likelihood of failure and help organizations design and optimize their cloud environments for cost and performance.

## Findings

Successful cloud migrations rely on extensive coordination between business units and IT operations to identify benefits and drawbacks and align migration projects with business requirements. Before beginning a cloud migration, comprehensive planning is essential. Planning activities should include a full assessment of business functions, practices, and activities, an evaluation of internal IT services and systems, and their current and future system requirements. Using each system’s detailed requirements, organizations must then identify a comprehensive cloud strategy for the entire organization and each system selected for migration. Cloud strategies must include a well-thought-out approach to cloud types, services, and capabilities as part of a methodology selection process. Required resources and expected outcomes for migrating IT services to the cloud should be consolidated into a business case that identifies the approach, methodology, scope, timeline, and budget for cloud migration.

Once approved, cloud migrations must be executed with due diligence and care to avoid potential pitfalls in migration, including service disruptions, cost overruns, and project delays. Following migration activities, the organization must exercise additional caution to prevent outages or service interruptions caused during the cutover. Throughout the migration process, it is critical for IT and business units to monitor migration activities and ensure changes to the IT environment do not impact business operations.

Before and during a cloud migration, organizations must also remain mindful of critical challenges to cloud migrations, including security implications, vendor lock, legacy system migration, and cost management. Each challenge on its own could spell disaster for a cloud migration project, and careful consideration should be given to pre-empt any potential problems. A common source of cloud migration failures stems from a poorly identified cloud strategy and planning, a lack of adequate skills or expertise on the cloud migration team, and rushing to migrate critical systems to the cloud without adequately evaluating and testing prerequisite IT services and systems along with testing of IT services supporting business systems before moving them to production in the cloud environment.

## Recommendations

The substantial impact of IT operations on a business's ability to successfully execute its business functions and processes and provide business services to its customers requires every cloud migration to be meticulously planned and executed with due care and diligence. Figure 1 below provides a sample structure for a cloud migration process. A successful cloud migration relies heavily on identifying business needs and planning. Maximizing organizational ROI and minimizing organizational risk for cloud services requires careful consideration of existing and future business needs and alignment of cloud services with business goals.

Based on industry experience and internal experiences with cloud migration activities, we recommend spending significant time and resources crafting a well-defined plan. When in-house cloud expertise is insufficient, organizations should seek consulting services throughout the migration process to ensure all facets of the migration are carefully evaluated and considered. One tiny oversight can potentially have significant implications for a cloud migration project. By leveraging trained and experienced IT professionals or consulting services, organizations seeking to move workloads to the cloud are more likely to complete their migration with minimal impact on business operations and ensure that key challenges are identified and mitigated ahead of time.

Figure - Sample Cloud Migration Process

References

Andrikopoulos, V., Binz, T., Leymann, F., & Strauch, S. (2013). How to adapt applications for the Cloud environment: Challenges and solutions in migrating applications to the Cloud. *Computing, 95*, 493-535. doi:10.1007/s00607-012-0248-2

Baarz, M. (2020, May 6). *Confusion in the Cloud: Greenfield or Brownfield?* Retrieved from Capgemini: https://www.capgemini.com/se-en/2020/05/confusion-in-the-cloud-greenfield-or-brownfield/

DevOpsGroup. (2021, September 10). *3 reasons cloud migrations fail (and how to make sure yours doesn’t)*. Retrieved from DevOpsGroup: https://www.devopsgroup.com/blog/3-reasons-cloud-migrations-fail-and-how-to-make-sure-yours-doesnt/

Fahmideh, M., Low, G., Beydoun, G., & Daneshgar, F. (2016). Cloud Migration Process A Survey Evaluation Framework and Open Challenges. *Journal of Systems and Software, 120*, 31-69. doi:10.48550/arXiv.2004.10725

Gholami, M. F., Daneshgar, F., Beydoun, G., & Rabhi, F. (2017). Challenges in migrating legacy software systems to the cloud — an empirical study. *Information Systems*, 100-113. doi:10.1016/j.is.2017.03.008

Iqbal, A., & Colomo-Palacios, R. (2019). Key Opportunities and Challenges of Data Migration in Cloud: Results from a Multivocal Literature Review. *Procedia Computer Science.* *164*, pp. 48-55. Halden: Elsevier B.V. doi:10.1016/j.procs.2019.12.153

ORock Technologies. (2021, January). *A Practical Guide to Mission-Critical Cloud Computing*. Retrieved from Orock Technologies: https://go.orocktech.com/Mission-Critical\_Cloud\_Computing

ORock Technologies. (2022). *For the Healthcare Industry, It’s (Past) Time To Modernize Your Storage Solution*. Retrieved from ORock Technologies: https://go.orocktech.com/Healthcare\_Time\_to\_Modernize

Perry, Y. (2021, May 30). *What is Cloud Migration? Strategy, Process and Tools*. Retrieved from NetApp: https://cloud.netapp.com/blog/cloud-migration-strategy-challenges-and-steps

Rimol, M. (2022, April 19). *Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly $500 Billion in 2022*. Retrieved from Gartner: https://www.gartner.com/en/newsroom/press-releases/2022-04-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-500-billion-in-2022

SambaNova Systems. (2021). *Accelerated Computing with a Reconfigurable Dataflow Architecture*. Retrieved from SambaNova Systems: https://sambanova.ai/wp-content/uploads/2021/04/SambaNova\_Accelerated-Computing-with-a-Reconfigurable-Dataflow-Architecture\_Whitepaper\_English.pdf

Threat Stack. (2022). *7 Factors to Help You Choose the Right Cloud Service Provider*. Retrieved from Threat Stack: https://www.threatstack.com/blog/7-factors-to-help-you-choose-the-right-cloud-service-provider

Wilson, J. (2019). *The Bi-Directional Cloud Highway:User Attitudes about Securing Hybrid- and Multi-Cloud Environments.* London: IHS Markit. Retrieved from https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/ar-2019-ihsm-fortinet-wp-q2.pdf