HBR
CONSULTING

# Planning a Cloud Migration?
# Practical Considerations for Law Firms

hbrconsulting.com | info@hbrconsulting.com | 312.201.8400


advisory | managed services | software solutions | insights

# Table of Contents

## Introduction

Cloud migration offers both benefits and challenges. A recent Forrester survey asked about perceived challenges in cloud migration and actual challenges experienced. The primary challenges respondents cited were security, privacy and network design. If successful, however, cloud migration can improve each of those three areas. Respondents also cited several improvements offered by the cloud: a faster time to deploy, quick and easy scaling, ease of administration and outsourcing as improved tasks. Cost should not be the reason for a cloud migration. Migration rarely generates savings, although it can be used to avoid significant data center capital expenses. Cost savings typically occur when a business is considering reinvesting in a new data center or a refresh. In a cloud migration, if not planned correctly, the unpredictability of cost can become a nightmare.

Despite some of their initial reluctance, law firms are increasingly moving to the cloud. The current remote working environment has augmented firms' interest because of the increased accessibility of various applications. Our prior whitepapers, Forecast: Law Firms Will Be Cloud Ready By 2021 and Law Firm Cloud Strategy: More Than "Cloud First," describe some of the strategic issues for law firms' cloud migrations. This whitepaper discusses the details of the actual migration of applications to the cloud. A successful cloud migration involves several considerations: strategic business considerations; planning and budgeting; cloud readiness; adoption (the actual migration); and governance. Each of those is discussed more fully below.

## Strategic Business Considerations

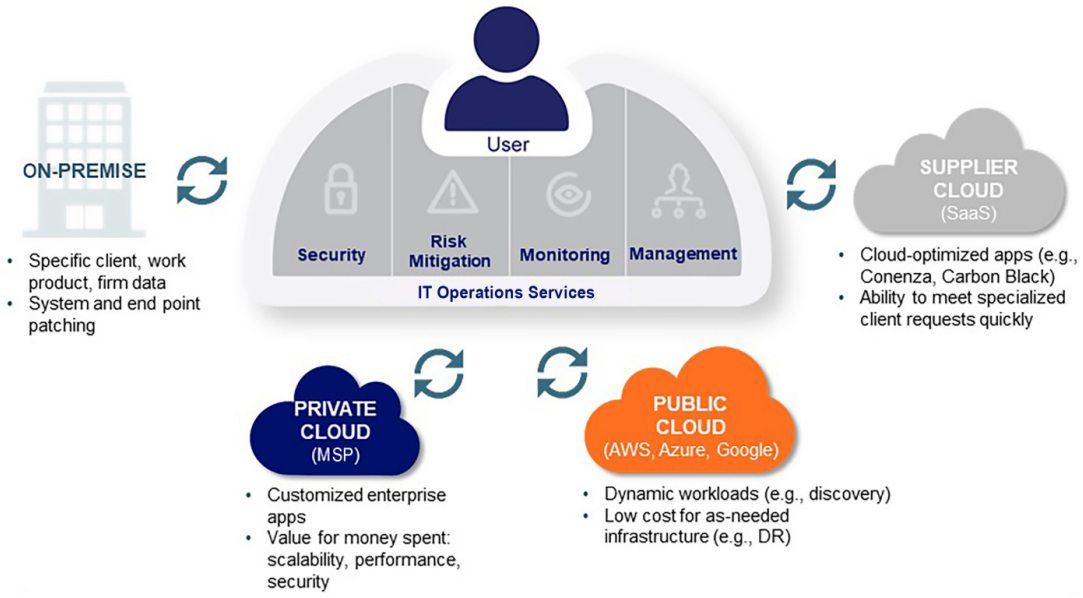
There are a number of business considerations firms should examine when determining which cloud platform best suits their business needs. Several of those are discussed below.

1. **Match the right workload requirements for each application that is a candidate for cloud migration**. For every application you are considering moving to the cloud, it is important to understand the workload requirements. Where is the application's data stored, how is the data accessed and what data compliance requirements must be upheld? How is your product licensed?
   Is it cloud (remote access) friendly? Can each workload scale vertically and horizontally? Vertical scaling ("scaling up") adds more power among the systems you have, while horizontal scaling ("scaling out") adds more machines. How can you best mitigate latency and performance issues?

2. **Choose a platform option: private, public or hybrid.** The key element of the platform selection equation is the business' requirements. However, it should be noted that the choice between public, private and hybrid solutions does not mean exclusive use of one option at all times. As time goes by, the business needs may change, and that may impact the cloud solution of choice. How might your investments change over time (capital versus operating expenses)?

- **Private Cloud**: Used by a single organization and not exposed to the general public. A private cloud resides inside the organization, behind a firewall. A private cloud can be quite expensive, since the organization itself must provide the hardware, applications and network.
- **Public Cloud**: A multi-tenant model in which a cloud service provider manages the services and the organization simply uses them. The provider supplies the hardware, sets up the application and provides the network accessibility according to the service level agreement (SLA).
- **Hybrid Cloud**: Includes the use of both private and cloud models, according to the requirements and capabilities of the applications and services delivered.

## CLOUD OPTIONS




3. **Address compliance requirements.** Your firm may have compliance requirements, such as laws and regulations that apply to using the cloud. When moving to the cloud, the country where your data is stored and accessed from determines what laws will apply, along with their impact.
4. **Consider user geography.** Emerging compliance requirements can also direct data residency and/or localization for businesses. Some applications can adapt to these requirements better than others. For example, Microsoft Office 365 will allow a firm to centralize tenant location, allowing multiple satellite locations and facilitating fluid management of data restrictions, balancing both compliance and user experience.
5. **Align cloud service provider agreements.** It is important to match provider agreements with your firm's business requirements. These agreements, often called Cloud Service Agreements (CSAs), can be inflexible. The agreements generally include three sections: Customer Agreement, Acceptable Use, and Service Level. The Customer Agreement section includes

the processes and procedures used by the platform provider, role and responsibility definitions. An Acceptable Use Policy (AUP) prohibits use activities that are improper or outright illegal. The SLA describes levels relating to availability, serviceability, or performance, including thresholds and financial penalties.

6. **Understand data storage concerns.** Cloud storage can be used to protect against the business interruption risks posed by natural disasters, with backups located around the globe. In 2020, online data backup has been documented to cost about $12 per 10 GB of data. Hidden concerns are:

    - **Compounding Storage Size**. Retaining backup copies for human error protection, natural disasters and system failures, as well as to meet various regulatory requirements can compound storage size.
    - **Retrieval Fees**. Cloud offerings are often cold storage, which could charge a retrieval fee to users who need to access their data. Be mindful of these types of fees.
    - **Network Egress Fees**. Cloud platforms allow you to upload data for free (ingress), but moving data out (egress) initiates fees that vary greatly based on amount of data and geography where the data resides. (Beyond egress fees, uploading or downloading can also be restricted by your WAN connection, where a transfer of multiple TBs can take a long time.) Always be mindful of this primary cost. Depending on data usage and need, network egress fees can significantly impact decisions for data management and should be considered when determining data residency.
    - **SLAs**. Does your cloud provider offer features to meet your firm's backup and retention policies? What are its guarantees for recovery time and uptime? Ensure your firm maintains data sovereignty requirements.

> The choice between public, private and hybrid solutions does not mean exclusive use of one option at all times.

## Planning and Budgeting

The most important consideration in cloud migration is planning. With strong planning, the actual migration will be relatively easy. Without strong planning, you may find yourself suffering buyer's remorse.

### Planning Cloud Migration

Cloud migration has been defined by Technopedia.com as:

> …the process of partially or completely deploying an organization's digital assets, services, IT resources, or applications to the cloud. The migrated assets are accessible behind the cloud's firewall. Cloud migration is also known as business process outsourcing (BPO), which may entail migrating an entire organizational infrastructure, where computing, storage, software, and platform services are transferred to the cloud for access.

Most legal professionals associate the cloud with a software-as-a-service (SaaS) solution. SaaS solutions offer a full portfolio of capabilities specifically written to take advantage of the cloud and its offerings. Another approach to the cloud is to rearchitect a current on-premise application for the cloud by mitigating performance issues and modernizing the user experience. The benefits of cloud computing, such as performance and lowering costs, could be lost without proper planning, such as over-procured machines, unplanned security tools and large data egress trends.

### Planning Security

A clear and transparent relationship with a platform provider that follows standards such as SSAE 16, SOC 2 or ISO 27001 is the best strategy to manage cloud compliance. Approach cloud at a technical level using publications such as those from the National Institute of Standards and Technology (NIST). This will assist you in vetted best practices and protections.

**Control continuous change.** Develop standards for configuring all system components, addressing all known security vulnerabilities with industry-accepted system hardening standards. The cloud platform will also be standardizing its offerings, evolving over time. Be aware of these changes to ensure your environment is not negatively affected by them—for example, that they do not cause emergency updates or have other adverse effects.

**Establish trusted zones.** Segmentation between virtual machines (VMs) is relevant to configuration and maintenance. Configure the management network to restrict access only to known and trusted endpoints. An attacker will likely target the management interface to gain privileged access, so hardening and segmenting this interface is crucial to maintaining data security.

The benefits of cloud computing, such as performance and lowering costs, could be lost without proper planning, such as over-procured machines, unplanned security tools and large data egress trends.

### Planning Connectivity

In addition to choosing your platform options, some applications place high demands on data transmission between the cloud and the on-premise network. Firms can choose the cloud connection that best meets their needs. Options include MPLS, direct and internet.

**MPLS**. High-performance and private connections from the firm's network to the cloud. Bandwidths range between 50 MB to 10 GB. managed service with end-to-end responsibility and SLAs, short connection times, high security and flexible contract periods.

**Direct.** You can choose an exclusive direct connection from the firm's network to the cloud data center. There are varying options depending on the cloud platform provider that include multi-client-capable connections with guaranteed high bandwidths at up to 100 GB and low latency.

**Internet.** Secure the firm's VPN to the cloud via the public internet, with managed security service for secure access to internet services.

### Budgeting and Workloads

The most critical step in this journey is to understand the total cost of ownership (TCO) to run the same workload on-premises compared to the cloud. This includes performing an in-depth discovery of the functionality of your application, including application maintenance, data protection and any security requirements. Early in this process, you should establish a standard resource unit to normalize the data (for example, Total vCPUs +Total RAM / #VMs). The investments in cloud platforms can be significantly different.

A projected growth rate model also needs to be performed for your workload. A higher growth percentage calls for greater reliance on standardization and automation to reduce overall costs at scale. Low-growth workloads are not the best fit for the cloud because the firm will not see the cost savings compared to an in-demand application that utilizes the cloud's elasticity and on-demand nature.

> Avoid vendor lock-in: weigh the pros and cons of each service and consider the extent to which you plan to use their catalog of offerings.

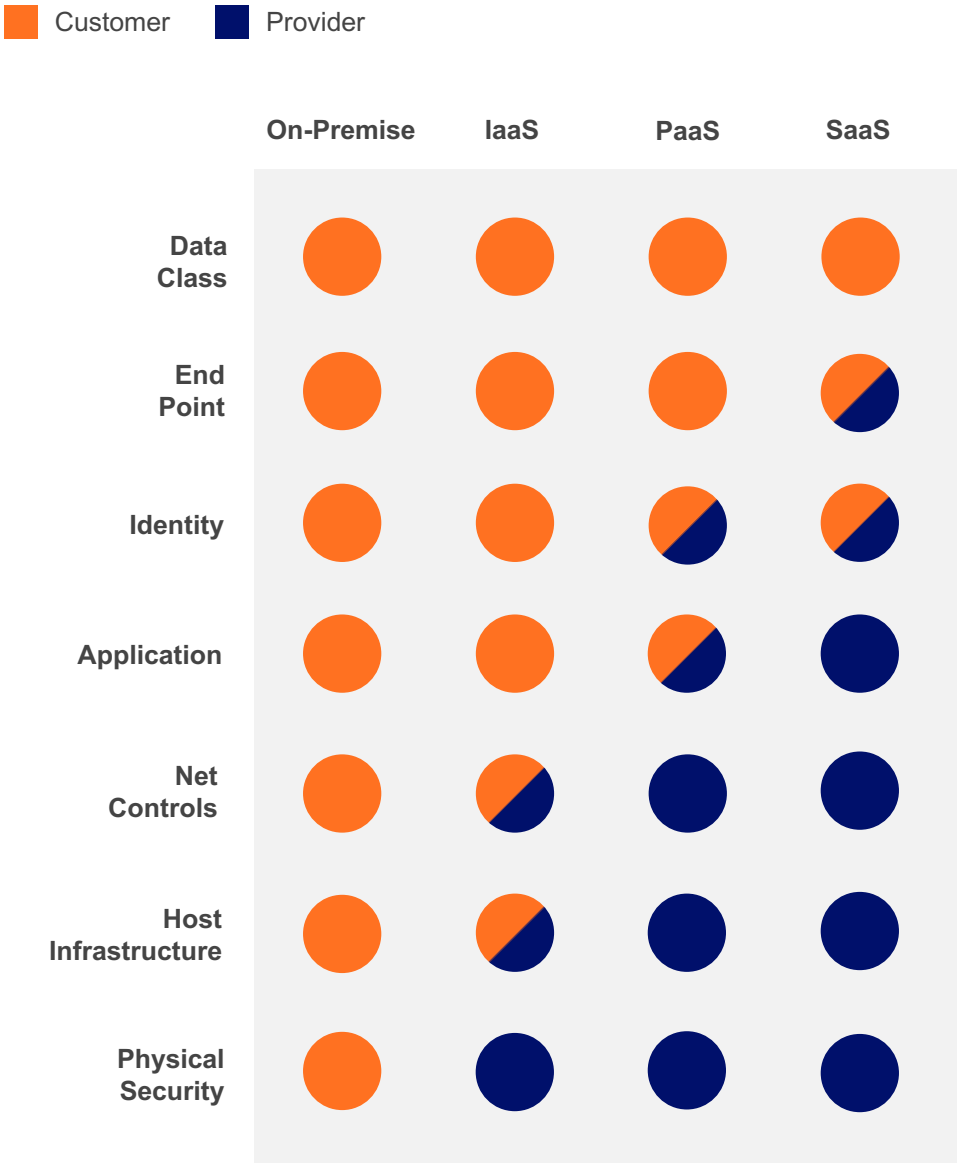
## Cloud Readiness

Once you have planned and budgeted your cloud migration, take the steps necessary to prepare for the migration. A preliminary step includes verifying that the application supports a cloud-based licensing model. For data that will be stored in the cloud, ensure that all the layers adopt encryption best practices. Automation options improve productivity and eliminate possibilities of human error. The use of scripting and third-party tools can reduce the time required for infrastructure builds and updates to minutes instead of hours. These approaches can also avoid configuration drift, unintended vulnerabilities or other human error issues. Lastly, avoid vendor lock-in: weigh the pros and cons of each service and consider the extent to which you plan to use their catalog of offerings.

### Cloud Options

Law firms considering a cloud migration must decide whether to purchase a previously built SaaS product, rearchitect the application or run the application as is. The latter involves knowing your application workloads, dependencies and platform requirements to ensure that proper migration will not negatively affect user experience or data protection.

## CHART OF RESPONSIBILITY




There are three types of cloud platforms:

**Public cloud – no maintenance, near-unlimited scalability, high reliability.** In the public cloud, cloud servers, storage and other components are owned and operated by a third-party cloud service provider and delivered over the Internet (e.g., Microsoft Azure, Amazon Web Services [AWS]). In this platform, hardware, storage and network devices are shared, used for environments such as email, online applications, storage and testing environments. Public clouds are more susceptible to security threats because of their shared infrastructure and multiple access points. There is a shared responsibility where the security of the infrastructure is assigned to the platform provider, while the workload is the customer's responsibility. These platforms often operate on a "pay as you go" model. If you are committed, consider looking into one to three-year purchase terms to explore additional financial benefits.

**Private cloud – more flexibility, improved security, high scalability.** Resources used exclusively by one organization are called a private cloud. The private cloud can be physically located at the firm's on-site data center or with a third-party service provider. With increased control over the infrastructure, this option is typically more secure than a public platform. The firm has full responsibility for the effectiveness of its security policies and protocols. Private cloud is more expensive because you will need to purchase, rent, maintain and manage infrastructural resources.

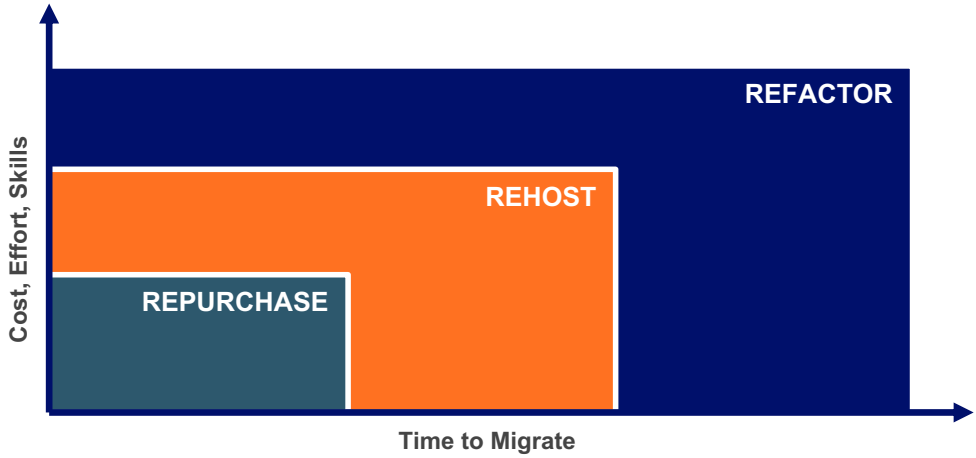
**Hybrid cloud – control, flexibility, cost-effectiveness, ease**. Often called "a safe choice," hybrid cloud combines on-premises infrastructure, private cloud and public clouds. In this environment, data and applications can move between private and public clouds for greater flexibility. As an example, public cloud can be used for high-volume, lower-security needs, and the private cloud or on-premises infrastructure for sensitive, business-critical operations. Since a hybrid option combines the use of both public and private clouds, security becomes more complex. The objective is to distribute the workload across both cloud platforms, maintaining compliance requirements and security policies while taking advantage of the specific advantages each platform has to offer. Hybrid cloud costs combine "pay as you go" and private cloud expenses. This is typically the most cost-effective option, allowing you to manage the workload according to need. Hybrid allows a balance of operational expenses and scalable costs based on the situation.

### Application Maturity for the Cloud

With the advancement of technology stacks, cloud adoption is snowballing. Mobile devices have pushed businesses, including law firms, to retire their applications and replace them with modern, public and private cloud-based ones. Most firms are still saddled with a few critical applications that are difficult to completely migrate or update for the cloud.

Applications have varying degrees of readiness for the cloud and fall into three categories of migration maturity. Some are capable of being rehosted to cloud platforms directly, while others may need to be updated or replaced.

MATURITY MIGRATION STATE



### Microservices

If you can afford to break the development up into multiple teams, enabling you to deploy more quickly, microservices may be your best option. Microservices refers to an architecture comprised of small, modular and independently deployable services that are designed to be ultra-scalable and fault-tolerant to meet workload requirements.

These services are achieved by the business rearchitecting its applications from the core or writing all new with the microservices approach. Keep in mind, utilizing the capabilities of microservices could cause challenges with monitoring and troubleshooting, such as service disruptions, caching issues, network latency and database errors.

**Repurchase.** Some firms may decide to invest in another alternative application that is cloud friendly, replacing or upgrading it. Disposal, commissioning and decommissioning costs may be significant.

**Rehost (or Lift + Shift).** This process includes taking virtual machines currently running on-premises and "lifting + shifting" them to the cloud. Cloud providers such as AWS, Azure or Google Cloud, or at times a private data center configured as a private cloud, are perfect platforms for this option. These virtual machine configurations need to be well architected to ensure both performance results and budget costs are met.

If you have been dwelling in the hybrid environment too long, identify your assets that have the most substantial business impact and start focusing on application migration efforts for those assets. Cloud platforms with platform-as-a-service (PaaS) include new features and capabilities, opening a comprehensive library of tools where minor changes to legacy apps can bring unprecedented benefits.

**Refactoring Applications.** If the business realizes that its lifted + shifted applications are not delivered effectively from the cloud, then refactoring becomes the next option. These options include several platform-as-a-service (PaaS) technologies from companies such as Google, AWS and Azure, as well as many others. The cloud-native offerings become elastic, dynamically consuming computing resources to meet varying workloads. When refactoring apps, organizations can also include optional environments such as container technology, but also need to be mindful of vendor-lock, which could result in poorer application portability. Refactoring often leads to a full re-write long term, buying time for a business to introduce other changes to the application to best meet business objectives.

### Migration Tools and Skillsets

When law firms perform a cloud migration, it is important for IT to have the right tools to help the team monitor workloads and effects on the environment. A few examples of migration tools include the following:

- Microsoft Azure Advisor and AWS Trusted Advisor offers various optimization recommendations to help manage cost, performance and security.
- Azure Migrate tools assess VMware workload performance in an Azure public cloud before the migration. Azure Site Recovery helps move VMs to Azure.
- AWS Migration Hub helps monitor the progress of the migration, which includes displaying the status of all AWS portfolio resources. AWS Application Discovery Service maps the planning

stages of a migration. This includes providing insights about the configuration, dependencies, data utilization, etc.

- Google Cloud Storage Transfer Service moves data into the cloud. It also backs up data and moves it from one entity to another. Google Transfer Appliance works offline as a migration service for large data transfers.

Organization skill sets will also need to be adjusted. In addition to the traditional migration skillset and project management capabilities, more in-depth skillsets may be needed. These skillsets change based on the model of migration and the cloud environment being built, but typically include, but are not limited to:

- **Compute Operations.** Machine virtualization, cloud infrastructure and application monitoring tools and metrics.
- **Networking for Workloads.** Virtual networks, complexities of complicated workloads, perimeter network design, etc.
- **Cloud Integration.** REST APIs for third-party integrations, building .net applications, PowerShell, and a working understanding of code and script (Python, Perl, and Ruby).
- **Database.** Skills beyond what has been applied in the typical data center are needed for cloud operations. These skills include limitations with size, storage performance, database cloning and multi-cloud operations.
- **Security.** The threat surface of the cloud is vast and particularly vulnerable to attack. Datacenter security skills could be retained by ensuring external connections with firewalls and intrusion detection systems. Understanding the different risks here and using cost-effective native cloud options requires new learning.

> If you have planned your migration thoroughly, the migration process should go smoothly and quickly.

## Adoption

Once you have chosen the platform and developed a plan, it is time to perform the migration. Building the infrastructure to support the application is the next step. This process includes building servers, storage and network components to ensure workloads are supported and proper access is allocated.

Setting up the infrastructure can often be performed through automated deployment using scripts and templates. Scripts automate a more time-consuming “point click” in the native configuration interface. Templates are applied by choosing from the cloud platform's existing pre-packaged offerings.

### Avoiding Regret and Preparing for an Exit Strategy

You may discover that your application does not work as effectively in the cloud. There may be reduced latency or security issues, cost or other challenges. Law firms sometimes find that not all applications are a good fit for the cloud. It is our experience that detailed planning helps firms avoid these situations, but even after a thorough review you still may run into issues that require an exit strategy.

Having an Application Lifecycle Management (ALM) in place will make your exit strategy much easier. ALM covers the idea conception through development, testing, deployment, support and retirement. This includes tasks such as testing in the new environment before migration and double-checking potential compliance requirements.

When you must exit the cloud environment to which you have migrated, consider the changes that were made before the migration. Backing the application out to its original platform might be an option, or it might make sense to leave it in the cloud while seeking replacement solutions. Your firm need not return to its previous on-premises configuration, and progress could be made by taking a smaller step by moving to another cloud maturity level. Tools that calculate cloud cost can help law firms plan the cost of a cloud configuration before the migration.

### Performing the Migration

Most migration plans can be executed iteratively, starting with confirming the cloud architecture design. Setup includes network, security, storage and other base products and services. Next, move resources according to the identified priority and applying the dependency constraint. The application setup follows with a fully managed testing phase.

If you have planned your migration thoroughly, the migration process should go smoothly and quickly. It is essential not to ignore security during the migration, including temporary storage.

Following your migration, resource optimization and resources allocation, ensure your teams have a plan for distributing resources to your application.

### Transferring Data

Different methods can be used for copying everything over to the new cloud platform, depending on the storage size. You will also need to calculate how much bandwidth is necessary to make a move.

These methods include general copying from on-premise to the cloud network or, for static data, it is preferable to use physical media to expedite the migration process for file, block or object storage. Production data options include mirroring using synchronization to represent a full, up-to-date mirror copy.

### Transitioning the Workload

Focus on data performance, usage and stability following the migration process. Before moving the workload to production, perform stress-tests and optimization adjustments to meet performance requirements. Testing failure conditions, as well as redundant systems, ensures appropriately configured application security in the cloud.

### Following Up After the Migration

Follow up the migration by retiring the on-premises products and services recently migrated. Be sure to perform some type of shutdown: wait a period to ensure none of these components contain information required in the newly migrated environment. Retire the product or service permanently or follow any retention policy you have in place.

Be sure to have the proper management tools in place in the newly migrated cloud environment that consider factors such as health across the entire environment, application performance, governance and compliance requirements, and cost management.

## Governance

An effective cloud governance solution ensures risks of exposed data, non-compliance with policies or regulations, or cost overruns are well contained. Critical elements of governance include policies, identity, consistency and cost control.

With security requirements set, **policies** and enforcement can be easily applied across network, data and asset configurations.

The cloud offers the opportunity for **identity** to be consistently applied through access controls across the cloud instance.

**Consistency** and deployment acceleration will ensure greater effectiveness through the use of cloud platform tooling (i.e., scripts, templates) to manage risks such as onboarding, drift, discoverability and recovery.

Cost is a primary concern for cloud users. Develop policies for **cost control** across your cloud platform.

## Conclusion

Cloud computing offers many benefits, allowing increased access and scalability. Without a clear cloud strategy and migration plan, however, the negatives can quickly wipe out the benefits. It is critical to pay attention to the planning and ensuring readiness before proceeding with a cloud migration. Like many things in life, you will get out of the experience what you put in it.

## Connect With Our Experts

For more information regarding steps that your firm can take to advance its IT function, please contact one of our experts:

**Brian Clayton**
Senior Enterprise Architect

**O** 937.993.0308
**E** Brian.Clayton@hbrmts.com

HBR
CONSULTING

HBR Consulting (HBR) delivers advisory, managed services and software solutions that increase productivity and profitability, while mitigating risk for law firms, law departments and corporations. As trusted advisors with deep industry experience, clients partner with HBR to achieve significant, sustainable results.

hbrconsulting.com | info@hbrconsulting.com | 312.201.8400


advisory | managed services | software solutions | insights