Cloud Adoption

Putting the Cloud at the Heart of Business and IT Strategy
Executive Summary

Cloud computing is rapidly maturing. It can no longer be considered a fad or an emerging technology; it is now an intrinsic part of the enterprise landscape. Increasingly, cloud adoption is being driven by business transformation needs — not technology-centric decisions — as businesses respond to demands levied by rapidly evolving consumer behaviors, changing business models, and the need to respond to opportunities and risks from new market entrants. As such, chief information officers (CIOs) and chief technology officers (CTOs) are adopting cloud computing at an increasing pace to help their organizations face the future with confidence.

At the same time, CIOs and CTOs need to manage seamlessly this shift in the computing paradigm while operating under relentless regulatory pressure and dealing with increased data security and privacy requirements. They also face the challenge of managing aging and complex legacy IT infrastructure and system resiliency in today’s “do more with less” environment.

Technology executives should leverage cloud technology to address a number of business and technology objectives, including:

1. Supporting **business and IT transformation** in response to rapidly changing business models and new market entrants
2. **Focusing on their core business**, rather than IT infrastructure
3. Improving the **agility** and speed to market for new products and services
4. **Shifting capital expenditures (CAPEX) on large-scale data center build-outs to operational expenditures (OPEX)** aligned to business demand
5. Taking advantage of the cloud’s **elastic capacity** to support scaling up and down based on business demand
6. Capitalize on cloud service providers’ investments to **reduce and manage “technical debt”**
7. Leveraging cloud providers to deliver **improved resiliency and business continuity management capabilities**

This paper — the first in a series that delivers Protiviti’s perspectives on cloud adoption — provides advice from a CIO/CTO perspective on how to initiate and execute a comprehensive cloud computing strategy, with emphasis on four strategic components — strategy, implementation, security and service assurance — to help guide the cloud adoption process.
Linking Cloud to Business Strategy and IT Transformation

The big question that echoes across CIO and CTO offices is how to formulate a comprehensive cloud computing and adoption strategy. The first step is determining the goals and guiding principles to govern the execution of such a strategy. This must include an articulation of the risks to be considered and managed.

Firms of all sizes and across industries are adopting cloud technology. Where once some highly regulated industries were reticent to leverage cloud functionality for core operations, today there is an increased acceptance of cloud as a method to increase speed and flexibility as well as to manage costs. Industry context remains a critical consideration when developing a cloud strategy, however. For example, financial services firms, which are seeking to modernize their core computing platforms and digitize processes while fending off advances from new entrants such as fintech, or financial technology, companies, are perfect candidates for adopting cloud computing. However, their strategy must consider their regulatory environment.

Adopting cloud computing services is not an end to a project; it is a beginning and a new operating model for IT. By placing cloud at the center of a renewed business and IT strategy, firms can capitalize on the generated efficiencies and drive business success.

Before starting on this strategic journey, organizations need to understand their own business priorities within their specific industries and regulatory context. Such an exercise is essential when embarking on any technology design; only by placing technology design in the context of the individual firm can it enable true business and IT transformation.
Proactively Eliminating Barriers

There are a number of barriers to cloud adoption. Progressive organizations seek to identify and address them proactively. Barriers include data security and privacy, systems integration, service assurance, vendor management, so-called shadow IT and the need to support bimodal IT, among others.

Security and Privacy
Security and privacy concerns are often a principal barrier hindering cloud adoption for many firms, but security capabilities in the cloud have matured significantly in recent years, substantially eliminating this as an obstacle. However, a solid security and privacy strategy should be developed early on to enable cloud adoption, rather than hinder it. Solving security issues first gives the firm freedom to adopt cloud services confidently and to quickly enhance its offerings and grow its business faster than its competitors.

Systems Integration and Service Assurance
Most companies will not be able to migrate all their processing to the cloud, and they are likely to have multiple cloud service providers. Managing this hybrid environment with consistent service performance demands solid systems integration and service assurance capabilities. Defining these issues up front as part of the cloud adoption strategy is often a critical success factor.

Vendor Management
Vendor management is an absolutely critical concern in every cloud adoption strategy. Given the important role that cloud services will provide in a firm’s infrastructure, close attention must be paid to selecting the right partner(s), developing appropriate contractual terms, aligning service levels to delivery capabilities and effectively managing the supplier relationships over time.

Shadow IT
The strategy for managing shadow IT is often another critical issue. In this context, “shadow IT” refers to IT systems and IT solutions built and deployed by departments other than the IT function. They often harness business-aligned, tech-savvy resources to develop effective solutions, but they can also expose an organization to security, compliance and other operational risks. Limited visibility into the extent of shadow IT present in an organization can also pose significant challenges in understanding the full scope of cloud adoption. Developing and implementing a sound policy that balances risks and rewards of this equation is important, particularly in heavily regulated industries such as financial services.

Bimodal IT
In addition to hybrid operations, the reality of bimodal IT is becoming the typical pattern for many organizations. Bimodal IT is a concept that explains how organizations must support two distinct IT enterprise patterns: One is a more traditional IT model that focuses on stability and efficiency; the other is more experimental and agile, focused on time-to-market and rapid application evolution. Bimodal IT can be a management challenge, since the traditional IT function needs to be kept running while continuing to encourage agility (which is frequently driven or supported by cloud deployments). Designing and implementing a strategy that supports both is very often required.

---

Not all clouds are created equal. Some cloud providers are more mature than others in all respects — security, compliance, audit ability and services assurance. Selecting the appropriate provider is critical. Firms also need to consider the three main cloud deployment options: public cloud, private cloud and hybrid cloud:

The **public cloud** is operated by one or more partner providers and shared among users across different organizations. It promises the highest level of scalability.

The **private cloud** is operated solely for a single organization and can be located on or off the premises. It can be highly customized and dedicated to each company’s needs.

The **hybrid cloud**, a combination of the public and private clouds, promises to harness the best of both worlds but demands orchestration between cloud platforms.

Cloud service models are also categorized by how services they provide are consumed:

**Software as a service (SaaS)**, sometimes referred to as on-demand software, gives users access to application software in return for a subscription fee.

**Infrastructure as a service (IaaS)** provides hardware technology services, such as virtual machines, storage and networking.

**Platform as a service (PaaS)** typically offers a preconfigured operating environment for firms to focus on developing and testing new applications and services. This helps to cut costs and to reduce the complexity of buying and managing the underlying hardware and software layers.

When creating a cloud adoption strategy, companies need to consider carefully the profile of their business services, implementation efforts, service delivery integration, and security and privacy risk appetite. These requirements should then be used to determine the right cloud deployment options and service model. It is important to keep in mind that an enterprise will often adopt different variations based on workload characteristics. Without a complete and balanced approach to cloud adoption, firms would not be able to maximize the benefits of cloud computing and could further add to technical debt.
Cloud Implementation Success

A successful cloud adoption has four distinct components: strategy, implementation, service assurance and security — with linkage to legacy systems where necessary.

- - - Considerations for Cloud Computing
Strategy

Cloud computing strategy is about deploying the right application services on the right architecture, based on the risk appetite of the organization. The strategy will often require a different way of designing, deploying and managing IT services. This process is usually not as simple as migrating from an existing technology platform to the cloud. There are several strategic considerations to evaluate first:

- **Architecture.** The development of a comprehensive cloud architecture seeks to transform application capabilities and services into component designs to reap the full benefits of cloud computing, including agility, scalability and availability.

- **Governance.** Most enterprises should implement a holistic cloud governance structure to guide and rationalize application services deployed onto the cloud in a risk-sensitive, secure, economical and compliant manner.

- **Deployment Readiness.** Organizations need to determine whether their existing application services are sufficiently componentized to be able to take advantage of service-oriented architecture (SOA), application programming interfaces (APIs), cloud computing models (CCMs) and other leading standards.\(^2\)

- **Platform Integration.** Firms need to ensure that their cloud adoption strategy contemplates the full breadth and depth of their environment. As noted earlier, it is likely that this will be a hybrid environment with legacy systems, multiple cloud providers and, in many cases, application service providers (ASPs). Systems integration patterns are often critical in a hybrid environment.

Implementation

The implementation of the cloud and the day-to-day management of cloud operations should be owned by the organization’s service operations function to ensure issue resolution and minimal disruption of the technology stack. This function needs to focus on the following essential areas:

- **Risk Management.** An effective risk management program is critical to the success of any IT implementation project. This should involve conducting a continuous and/or proactive risk assessment to ensure that data integrity, data privacy, regulatory compliance, data segregation, vendor due diligence and third-party disclosures are all being managed appropriately.

- **Capacity and Operational Excellence.** The use of current technology components must be optimized to ensure that agreed service levels are provided to the customers in an economical way. Equally important is the due diligence and capacity planning discipline required to better anticipate peak and growing workload demands. Operational excellence revolves around ensuring that robust processes are in place for enterprisewide systems that provide reliable data, which are immediately available with easy access to incident reporting and performance monitoring tools for the maintenance and support teams. Current policies should also be extended to provide coverage for cloud activities where possible.

• **Vendor Selection.** Organizations need to consider if they are being locked into a proprietary framework and/or platform with the cloud service provider. Future and current vendor contracts must be coordinated and managed according to enterprise risk management standards to ensure that the proper scope and the service level agreement (SLA) have been clearly defined and are aligned to the expectations of the technology owners.

**Service Assurance**

To safeguard cloud services, firms need a strong service assurance function, which may require their core legacy systems to be modernized or refreshed.

• **Core Refresh.** Legacy applications tend to be tightly coupled with limited code reuse, and certain application services may not be ready for deployment to the cloud. Cloud adoption presents the unique opportunity for organizations to redesign their application architecture to address such challenges through SOAs and APIs, to decouple links across the technology stack and to encourage the reuse of legacy code. However, these efforts must carefully consider quality of service requirements.

• **Platform Interoperability and Vendor Management.** Both IT customers and consumers expect seamless delivery of services and products. The IT function has to reinvent itself as the “service broker” that can navigate between cloud and noncloud platforms with confidence in order to orchestrate delivery of the best available services to its end users.

• **Data Portability.** Legacy data conforms to corporate policies and standards, whereas cloud data often does not or cannot. Additional challenges that need to be addressed include data encryption applied by cloud service providers, as well as data latency.

**Security**

The allure and advantages of cloud computing are often overshadowed by the notion that an organization has to forgo security to fully leverage the power of the cloud. As part of a heavily regulated industry, financial institutions are indeed faced with unique security challenges when considering a move to the cloud. In a recent survey, 28 percent of financial institutions said that they felt moving to the cloud had not only improved security but also reduced the risks they faced prior to implementation. Security remains a major concern, however, and organizations need to carefully consider this during the cloud implementation process.

• **Data and Privacy.** Protecting confidential and regulated data is a fundamental responsibility of financial services organizations. Firms therefore need to consider certain safeguards. Encryption remains the primary method of achieving compliance, while user behavior analytics is the leading method of identifying risky behavior. Organizations using public clouds should also consider the security of shared client infrastructure and/or applications, as well as where data may reside in the cloud and what regional privacy, disclosure and other laws might apply.

---

• **Access Management.** Protecting a cloud platform begins with managing access to it. Firms need to first determine user entitlement: Who has access to the cloud and how is that access is granted? Role-based access also needs to be considered. This is where firms manage user access through the creation of user groups and associating job functions to those groups. Leading practices include the use of single sign-on solutions for SaaS integrations. Firms also need to ensure that there is multifactor authentication in place that requires multiple keys to gain access to the system or application.

• **Regulatory Compliance.** This can pose a challenge for cloud vendors in terms of multitenancy, cross-border data sharing, and outsourcing of regulatory and compliance requirements. Standardized controls or frameworks to facilitate data, identity management, information security and governance should be developed and embedded in the design and approach under strategy, implementation and service assurance. Periodic due diligence is also required to assess whether data security, vendor services and IT controls are up to date.

• **Incident Management.** Firms need to have an organized approach to addressing and managing the aftermath of a security breach or attack. The foremost considerations are response times and incident responsibility. How quickly the cloud provider alerts the institution to a security threat and takes action is paramount, which requires having one person in charge to assume responsibility for dealing with a breach or attack.
Cloud Adoption Scenarios and Associated Risks

With any transformation program, avoid pitfalls by considering all the possible scenarios beforehand. The six general scenarios summarized below provide an indication of some of the implementation risks associated with separate cloud adoption approaches.

**Runaway Shadow IT**: The use of unchecked cloud services proliferates the problem of shadow IT. A complex network system can be created when business lines bypass the formal IT function and procure multiple cloud vendors for different services. Shadow IT solutions are usually not in line with the organization's requirements for control, documentation, security and reliability policies, among others. Users also may not consider the broader role of cloud software within the organization or how to securely enter and remove data. A runaway shadow IT situation may be created, causing multiple IT governance and assurance risks.

**Analysis Paralysis**: For the more cautious company, ensuring that the cloud adoption approach is in strict alignment with the organization's architecture and security policies, as well as inspecting portability of the cloud over the changing data landscape, may delay cloud implementation to the point where the organization loses its first-to-market and agility advantages. Although firms are correct to analyze their requirements and expectations for cloud adoption, overanalysis creates paralysis and doubt within the organization. This places project momentum and resources at risk.

**“Go for IT”**: The polar opposite of the previous scenario is the go-for-IT approach, where there is the risk that security concerns have not been thoroughly considered. In private or hybrid cloud deployments, organizations may overestimate security or focus solely on agility. This approach may lead to security risks in data segregation, data loss prevention and/or data privacy. It could also result in the organization having multiple clouds with varying security risk profiles to monitor.

**Buyer's Remorse**: With any large-scale project that has multiple options, there is a chance that the organization opts for the wrong solution. One particular scenario is when a firm has not adequately considered data operability of the cloud with legacy systems or the decoupling that needs to be completed in the technology stack. Such a situation would require many manual workarounds, while the delivery of services and products would be fragmented. Subsequently, services to end users between cloud and noncloud platforms would differ in quality.

**Cloud Experimentation**: The IT function needs to be heavily involved in any cloud adoption strategy, but there is a risk that IT begins to dictate cloud requirements rather than develop them in conjunction with the business. This approach can lead to the company adopting cloud solutions through continuous experimentation with noncore services. Cloud adoption must be strategically adopted by the entire organization; otherwise, the operational and cost-saving benefits of the cloud may be missed.

**Strategic Approach**: This is the ideal scenario for cloud adoption, in which the organization takes a comprehensive approach to cloud deployment. This approach incorporates extensive planning for all four cloud adoption components — strategy, implementation, security and service assurance — as well as considering how cloud services interact with the legacy technology stack. A thorough consideration of these four components during the planning process would mitigate the risks associated with shadow IT, a lack of data governance and security issues. However, the organization must continually evaluate the value the cloud delivers to business objectives.
<table>
<thead>
<tr>
<th>Approach</th>
<th>Profile Information</th>
<th>Implementation Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Runaway Shadow IT</td>
<td>Business may bypass formal IT and procure multiple cloud vendors for different services, resulting in a complex network system</td>
<td>Provisioning services without architecture oversight may give rise to &quot;skill strain&quot; on resources</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A runaway shadow IT situation may result</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Technology managed by the business may have inconsistent governance and poses service assurance risk</td>
</tr>
<tr>
<td>Analysis Paralysis</td>
<td>Strict alignment with organization architecture and security policies and inspecting portability over changing data landscape may delay implementation of cloud</td>
<td>First-to-market and agility advantages may be hampered or obsolete if analysis is conducted on aged cloud solutions</td>
</tr>
<tr>
<td>&quot;Go for IT&quot;</td>
<td>In private or hybrid cloud deployments, organizations may overestimate security or focus solely on agility</td>
<td>Security risk owned by the organization may include: • Data segregation • Data loss prevention • Multiple clouds to monitor • Data privacy</td>
</tr>
<tr>
<td>Buyer's Remorse</td>
<td>Insufficient consideration of data interoperability with legacy systems, as well as decoupling that needs to be done in the technology stack</td>
<td>Delivery of services and products will not be seamless, resulting in manual workarounds</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Services to end users between cloud and noncloud platforms will vary in quality</td>
</tr>
<tr>
<td>Cloud Experimentation</td>
<td>IT heavily dictating cloud requirements leads to company adopting cloud solutions through continuous experimentation with noncore services</td>
<td>Forgo operational and cost-savings benefits by not strategically adopting cloud</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Continued maintenance of unmodernized legacy technology core with decreasing marginal benefit</td>
</tr>
<tr>
<td>Strategic Approach</td>
<td>A comprehensive approach to a cloud deployment would incorporate planning for all four quadrants as well as interactions with the legacy technology stack</td>
<td>Strategy, security, implementation and service assurance planning would mitigate the risks associated with shadow IT, lack of data governance and security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Organization must continually evaluate the value cloud delivers to business objectives</td>
</tr>
</tbody>
</table>
Conclusion

Cloud computing adoption is not solely an IT issue; it is a strategic business issue. Financial services firms are more often being referred to as technology companies, forging ahead with new customer-focused services from online banking to mobile payments, all of which require IT systems and programs. The pace of technological change has caused the piecemeal implementation of such systems, with business lines often adopting their own cloud services to ensure speedy implementation of in-demand services.

Taking a step back to consider the firm’s cloud computing adoption strategy is paramount to ensuring a successful and rapid adoption that fits with the firm’s strategic business model. Focusing on what the cloud needs to accomplish for the organization is the key driver toward discovering the right fit. A poor strategy will cause remedial work and require additional investment. Done right, cloud adoption can be a swift, secure and risk-based solution. For cloud adoption to succeed, it needs to be part of a broader, holistic strategy that transcends business and technology concerns but is solidly grounded in IT.
Protiviti experts are strategists and transformation enablers who leverage cloud computing effectively to enhance business strategy.

Protiviti designs, develops and implements pragmatic, enterprise-class solutions that acknowledge the complexity of legacy and hybrid environments. Rarely is cloud the only solution in play for our clients.

Protiviti has a strong reputation in risk management, security and privacy, IT governance, and analytics and a loyal base of clients. We also seek to overlay a deep understanding of industry-specific concerns in our solution development. Our dedication to developing pragmatic solutions to address the real, underlying problems helps us produce value for our clients. This combination has made us a trusted partner to our clients.

Protiviti can assist companies with all four components that need to be addressed as part of a comprehensive cloud adoption strategy. Protiviti has deep domain knowledge and practical expertise with core modernization and IT transformation. Our experts have extensive experience with data privacy and IT security issues, including regulatory compliance and vendor network and security assessments.

Protiviti is able to guide companies through the entire cloud adoption process, from the development of a cloud security strategy and cloud architecture redesign to assisting with the development of a migration strategy and execution.

On a service assurance basis, Protiviti can help with designing SLA monitoring and reporting and disparate platform management, as well as recovery objective alignment.

Our goal is to ensure that firms adopt cloud computing swiftly and successfully as part of a considered, comprehensive and strategic development plan that keeps them one step ahead of the competition, while generating efficiencies and cost savings to the business that ultimately drive revenue growth.

We provide the following services:

- Core modernization
- Cloud architecture design
- Platform determination
- Data privacy and security
- Regulatory compliance
- Vendor network and security assessment
- Migration strategy
- Planning and execution
- SLA monitoring and reporting
- Disparate platform management
- Recovery objective alignment
ABOUT PROTIVITI

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 70 offices in over 20 countries.

We have served more than 60 percent of Fortune 1000® and 35 percent of Fortune Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

CONTACTS

Ed Page
Managing Director
+1.312.476.6093
ed.page@protiviti.com

Jeffrey Weber
Managing Director
+1.647.288.8505
jeffrey.weber@protiviti.com

Jonathan Wyatt
Managing Director
+44.20.7024.7522
jonathan.wyatt@protiviti.co.uk

ACKNOWLEDGEMENTS

David Lin, Randy Armknecht, Willis Zhang and Bennett Cotter contributed to the development of this white paper.