Executive Summary

One of the most important strategic issues IT decision-makers face is how to best leverage the rapidly evolving cloud resources available today. Those who make the right move could substantially improve the efficiency, reliability and flexibility with which they deliver critical IT services to their internal and external users.

Effectively migrating enterprise applications to the cloud means considering a number of salient points, including:

- Challenges and opportunities motivating organizations to consider cloud migration
- Key attributes and potential benefits of various cloud-provisioning options
- Issues and concerns faced by IT decision-makers regarding cloud migration
- The suitability of specific types of applications for cloud migration
- How to best ensure the success of a cloud migration project

With homework and a sound strategy, IT leaders should be empowered to make smarter decisions about migrating applications to the cloud, to act on those decisions with greater confidence and ultimately to achieve better results for the business.
The State of the Pre–Cloud Enterprise

IT organizations today are under intense pressure. On one hand, IT can deliver more value than ever when it comes to automating business operations, ensuring a great customer experience, capitalizing on new opportunities and pinpointing potential problems that require immediate attention. On the other hand, no organization has an unlimited IT budget. Every organization’s bottom-line performance relies, to some extent, on how well it leverages its finite IT resources to implement and run high-value enterprise applications.

A limited budget isn’t the only issue IT faces when it comes to enterprise applications. Other issues include the need to:

- Scale applications in terms of number of users, volume of data and other parameters despite the limited capacity of an in–house data center
- Ensure operational resiliency even in the event of data center disruptions such as hardware failures, regional power outages or extreme weather
- Allocate more IT resources to highly innovative and strategic projects – rather than simply keeping existing applications and infrastructure up and running

While these issues have become critical for IT decision-makers, cloud computing has emerged as a viable alternative to conventional application provisioning. Cloud computing decouples application provisioning from specific hardware and sometimes even from a specific data center. In doing so, it provides numerous benefits that align closely with the concerns noted above – as well as several additional benefits.

Because the cloud-computing model is so attractive, 90 percent of companies are already using the cloud in some form or another, according to a study by the Computing Technology Industry Association (CompTIA). And 69 percent of companies are planning to move at least some of their critical applications to the cloud by the end of 2014, according to research conducted by Virtustream.

Despite this powerful market momentum, many IT decision-makers still have serious questions that they need to answer before they move their applications to the cloud. These questions include:

- Will the enterprise be able to maintain the same standards for security and compliance?
- Will the performance of applications suffer as the result of a move to the cloud?
- Can applications in the cloud integrate and interoperate with each other as they do when they are running in the data center?
- Could any other unintended consequences result from a move to the cloud?

- How does the organization decide which applications to move to the cloud first – and which ones not to move at all?
- If and when the entity decides to move an application to the cloud, how can it do so with the least disruption and risk to mission and IT operations?

Clear, accurate answers to these questions are obviously a prerequisite for any successful move to the cloud.

The Cloud: What and Why

The term “cloud” refers to an alternative delivery model for traditional IT that can be hosted at an external service provider’s facility, on–premises in a company’s own data center, or both. Regardless of where it resides, infrastructure can generally be considered cloud if it possesses the following characteristics:

- **Metered**: Cloud computing is a metered technology that offers accurate calculation of CPU use. The process also serves to increase awareness among departments and users of the true costs associated with IT services. Keep in mind, while metered usage is part of the formal cloud definition, failure to charge for that isn’t necessarily an internal private cloud deal-breaker.

- **Elasticity**: Cloud environments should offer the ability to dynamically add or reduce computing capacity based on actual need and on demand. Typically, historical and real-time reporting provides stakeholders with visibility into fluctuations in both demand and the corresponding allocation of capacity.

- **Automation**: Virtualization offers the agility needed to speed up IT operations and trim costs by boosting infrastructure utilization. The self–managing aspects of autonomic computing automates the process by which the user can provision resources on-demand. Environments with these characteristics offer a wide range of benefits when it comes to the delivery of enterprise applications.

- **Reducing or aligning costs**: Cloud computing combines economies of scale with the ability to allocate computing capacity on an as–needed basis. This drives down the cost of provisioning enterprise applications – while also keeping those costs closely aligned with actual mission needs, even as those needs fluctuate over time. This reduction and alignment of IT costs is becoming increasingly important as organizations become more dependent on a growing portfolio of enterprise applications.

- **Scaling on demand**: Entities often experience periods of peak demand for their enterprise applications. Some peaks are predictable – such as those associated with end–of–quarter reporting or seasonal sales cycles. Others occur suddenly and unexpectedly due to the success of a marketing campaign or a disruption in the supply chain.
Under conventional provisioning models, organizations face a difficult choice when it comes to this peak demand: Either burn limited capital budgets on excess capacity to handle those peaks or endure subpar application performance until those peaks pass. Cloud computing eliminates this choice by making capacity available when it is actually needed without requiring the organization to pay for unnecessary capacity year-round.

- **Shifting Capital Expenditure (CAPEX) to Operational Expenditure (OPEX):** Chief financial officers have become increasingly aggressive about preserving capital. Cloud computing supports this financial imperative by allowing companies to avoid capital expenses on IT — to instead “rent” infrastructure on an as-needed basis from service providers as an operating expense.

- **Reallocating IT resources to strategic innovation:** Most organizations devote a high percentage of their IT budgets to maintaining operation of IT equipment, especially when it comes to ensuring the reliability of critical IT budgets to maintaining operation of IT equipment, increasing cost savings to maintaining operation of IT equipment. This spending severely limits their ability to allocate resources to new, innovative IT projects.

### Flavors of Cloud: Which Is Right for You?

While “cloud” generally describes any computing architecture that leverages virtualization and the resulting ease of provisioning resources, cloud implementations vary significantly in their suitability for different application workloads — and in their economics — based on how and where they are deployed.

Here are the key cloud “flavors” to consider:

<table>
<thead>
<tr>
<th>TYPE</th>
<th>DESCRIPTION</th>
<th>PROS</th>
<th>CONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hosted Public/ Multitenant</td>
<td>Service providers build large-scale cloud environments on infrastructure that is securely allocated to the application workloads of many different organizations.</td>
<td>Infrastructure is highly scalable. Operational burdens are offloaded. Economies of scale result in lower costs.</td>
<td>Multiple tenants bring potential for compliance and performance issues. Organization has less direct control of data and infrastructure.</td>
</tr>
<tr>
<td>Hosted Private</td>
<td>Service providers host cloud environments on infrastructure dedicated to specific applications, customers, industries, etc.</td>
<td>Combines scalability and operations offload with enhanced compliance, security and/or control.</td>
<td>Private cloud may not offer same economies of scale as public/multitenant cloud offerings.</td>
</tr>
<tr>
<td>Hybrid</td>
<td>Application workloads run in a combination of private- and hosted-cloud environments.</td>
<td>Allows for mixing and matching of different cloud flavors based on varying business and technical requirements.</td>
<td>Requires more sophisticated management and monitoring of application behavior and multiple cloud environments.</td>
</tr>
</tbody>
</table>

Cloud computing can free up these precious resources and promote innovation by reducing infrastructure costs and allowing operational burdens to be offloaded to service providers.

- **Leveling the playing field:** Due to their relative lack of capital IT budget and skilled IT staff, small to medium-sized organizations often struggle to implement the same technologies as their larger competitors. Cloud computing levels the playing field by giving smaller organizations access to the computing resources they need. In today’s market — where success often depends upon the effective use of state-of-the-art technology — this “democratized” access has proved to be a game changer.

- **Increased time to market:** With cloud computing, IT server provisioning, which can take six- to eight weeks, can be completed in a matter of hours. While cost savings and the ability to scale up and down are attractive, some organizations are pushed to the cloud by the ability to get products to market much more quickly.

Cloud computing offers other benefits as well. For example, economies of scale allow cloud service providers to build failover facilities more cost-efficiently than individual organizations can. This built-in infrastructure resiliency often makes the cloud an attractive way to safeguard business continuity. Those same economies of scale also often make it easier for service providers to engineer secure remote access to enterprise applications — making them an attractive choice for supporting mobile users as well as contractors and partners.

### Getting to the Cloud

While businesses can gain significant benefits by running their enterprise applications in the cloud, several key issues must be taken into consideration before doing so.

#### Application Suitability

Not all applications are architected to run in virtual or multitenant environments. In some cases, an application has intensive CPU or input/output needs that require a dedicated multithread processor and therefore don’t lend themselves to virtual machines that share physical CPU and I/O capacity with other applications.

In other cases, it may be because the application vendor has not structured the licensing of the application for a virtualized or multitenant environment.

Whatever the reason, IT decision-makers must first determine whether the application in question can run on a modern virtualized infrastructure “as is,” whether it must be modified to do so, or whether the cloud is totally out of the question because of specific technical limitations.
Network Requirements

When considering the use of hosted-cloud services, the network requirements of an application are a key consideration. This is because application traffic will have to travel a much different path than it does when the application is running in an enterprise data center.

For some applications — such as those designed to run as pure web browser–based services — this can be a nonissue. For others, network latency or jitter can be highly problematic. So the network tolerances of an application must be well understood before a cloud migration.

These tolerances are often complex. Many applications entail connectivity between multiple components such as a database, a middleware server, a presentation server and an authentication server.

These multiple network paths can all have implications when it comes to the end–to–end performance of an application. IT decision–makers must therefore factor in all of these paths when determining which application components, if any, can reside in the cloud and which ones need to remain in the enterprise data center.

The Need for Speed

When it comes to accessing public-cloud services, not all network connections are created equally. IT decision–makers therefore must carefully consider the tolerances of the application in question with regard to latency, jitter and other network characteristics — and balance those against the cost of enhanced network connectivity. This is true whether public-cloud services are being accessed directly from an in–house data center or from a service provider’s facility.

Three main types of network connections can be used to access public-cloud services:

<table>
<thead>
<tr>
<th>TYPE OF CONNECTION</th>
<th>ATTRIBUTES</th>
<th>COST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Internet VPN</td>
<td>The lowest common denominator for connections to a public-cloud service, subject to the variations associated with generic Internet connectivity.</td>
<td>Low to none, depending on bandwidth requirements</td>
</tr>
<tr>
<td>Multiprotocol label switching–enhanced</td>
<td>Enables “class of service” connectivity that insulates the performance of cloud connections from other less–critical Internet traffic.</td>
<td>Additional costs charged by service provider. May require some reconfiguration of internal network.</td>
</tr>
<tr>
<td>Direct connection</td>
<td>Access speeds substantially improved by dedicated connectivity to public-cloud service that bypasses the public Internet.</td>
<td>Premium pricing</td>
</tr>
</tbody>
</table>

That said, tight network tolerances are not necessarily a deal-breaker for cloud migration, since some cloud providers offer better network capabilities than others.

Security

Stakeholders — including line–of–business managers, compliance managers and customers — have legitimate concerns about the security of data that is allowed to reside outside the control and confines of an enterprise data center. IT decision–makers, therefore, have to carefully consider the security implications associated with running applications on a hosted–cloud infrastructure.

In particular, the security of cloud providers should be evaluated based on several criteria, including:

- **Encryption** of data, both in motion over the network and at rest in the storage environment
- **Access control** in terms of how users are authenticated and how granularly permissions can be granted or denied for different application–related privileges
- **Perimeter security** such as firewalls, intrusion detection, periodic penetration testing and other best practices
- **Physical security** to ensure that unauthorized personnel cannot gain direct access to servers and storage arrays where sensitive data resides

IT decision–makers should bear in mind that the real question at hand is not whether a given cloud provider’s environment fulfills some theoretical ideal of perfect security — but rather whether it is more or less secure than other provisioning options.

Keep in mind, no IT environment is perfectly secure, but cloud provider environments are often much more secure than their enterprise counterparts because they are newer, more homogeneous and operate at economies of scale that allow for more intensive security operations.

Compliance

Many organizations operate under regulatory constraints that mandate how certain types of data must be managed and protected. This obviously has implications when it comes to provisioning applications in the cloud, because that provisioning will directly affect both where data is stored and where it moves while in use.

In some cases, regulations may make it impractical to move an application to the cloud. Companies operating in several countries, for example, may be subject to local regulations that forbid certain types of data from crossing national borders. This may make it necessary to keep data in separate, dedicated physical servers in each country where the company operates. These data centers may leverage virtualization — and may even individually utilize cloud–like computing infrastructure. But they will not be able to dynamically share computing capacity across all territories where the company operates.
In other cases, regulatory mandates may affect the choice of cloud service providers. Examples of such regulations include:

- **Health Insurance Portability and Accountability Act (HIPAA)**: A federal law that includes provisions that companies involved in healthcare must follow regarding the security and privacy of patient data.
- **Payment Card Industry Data Security Standard (PCI DSS)**: A set of requirements designed to ensure that all companies processing, storing or transmitting credit card information maintain adequate security.
- **Federal Risk and Authorization Management Program (FedRAMP)**: A program that standardizes how government agencies and contractors address cloud security assessment, authorization and monitoring.

These regulations affect application deployment in the cloud differently. PCI and FedRAMP, for example, provide criteria for certifying cloud service providers. An organization operating under either of those mandates, and looking to move applications to the cloud, could readily fulfill its compliance requirements by choosing a certified partner.

HIPAA, on the other hand, does not specifically define any technical certification for cloud service providers. Instead, cloud service providers confident of their ability to fulfill the requirements of HIPAA offer customers in the healthcare industry a Business Associate Agreement (BAA), through which the service provider agrees to both fulfill the data privacy requirements of the mandate and assume liability for any breaches. This shields healthcare companies from the financial and legal risks associated with data security breaches — although it does not necessarily mitigate the reputational risks associated with such an event.

### Service Level Management

When applications run on conventional infrastructure within an organization's own data center, service level management — while it can be somewhat challenging technically — is nonetheless relatively simple in principle. Applications run over known infrastructure components that are under the direct control of the company's IT staff. So if a problem arises, that infrastructure can be quickly assessed to determine the cause of the problem.

Things get a bit more complicated with in-house cloud environments because the infrastructure underlying an application is more fluid. This fluidity can make problems more difficult to diagnose and resolve.

The challenge is ensuring the level of service which changes dramatically when an application is running on public-cloud infrastructure. For one thing, the organization and the service provider must both clearly define what constitutes satisfactory performance in a complete and unambiguous service-level agreement.

The SLA should define not only expectations regarding the technical performance of the application, but also response times promised by the service provider in the event of a problem. A well-designed SLA will also define the roles and responsibilities of each party in resolving problems — as well as the consequences if conditions are not met.

---

**Service models and skills**

Cloud service providers offer several models for running enterprise applications on their hosted, virtualized infrastructure. These models differ significantly in many ways, including how they impact the skill sets required to use them. The following chart offers a general overview of service models available and their comparative impact on IT staff skills.

<table>
<thead>
<tr>
<th>SERVICE MODEL</th>
<th>ACRONYM</th>
<th>DESCRIPTION</th>
<th>BENEFITS</th>
<th>SKILLS IMPACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software as a Service</td>
<td>SaaS</td>
<td>Service provider manages all aspects of application provisioning, from underlying hardware to ongoing software updates.</td>
<td>All responsibilities for the application are offloaded to the service provider. Customization of the application is limited to configuration capabilities made available from the provider.</td>
<td>Little to none: May need to learn some configuration tools.</td>
</tr>
<tr>
<td>Platform as a Service</td>
<td>PaaS</td>
<td>Service provider manages the complete underlying technology “stack,” up to but not including an application itself: hardware, operating system, hypervisor, etc.</td>
<td>Provides access to scalable capacity and offloads bulk of IT management responsibilities while still allowing full control over enterprise applications.</td>
<td>Minor to significant: The service provider may use different technologies (such as a different hypervisor) with which IT staff are unfamiliar.</td>
</tr>
<tr>
<td>Infrastructure as a Service</td>
<td>IaaS</td>
<td>Service provider manages only the hardware infrastructure.</td>
<td>Provides access to scalable capacity and offloads some IT management responsibilities while still allowing full control over enterprise applications, hypervisors, operating systems, etc.</td>
<td>Minor: Requires use of remote management and monitoring tools.</td>
</tr>
</tbody>
</table>
Of particular importance is how problems are reported, tracked, resolved and then reviewed periodically to determine if both parties’ expectations are being met. Ideally, these processes should be sufficiently automated, which may entail some integration between the two parties’ IT help desks or trouble-ticket systems.

**Pricing**

Cost is obviously a primary consideration for any company engaging with a cloud service provider. But determining the cost of a cloud engagement can be tricky given the fact that service providers offer pricing structures that differ considerably.

In addition, the long-term cost of any cloud engagement can be difficult to estimate, because it is by definition tied to usage, which can be difficult to predict. Organizations should also take steps to ensure that they do not accidentally run up excessive charges due to unnecessary or unauthorized usage.

IT shops should consider other costs related to the cloud as well. For example, while an organization retains ownership of the data it generates over time in the cloud, cloud providers may charge a fee for the bulk transfer of that data. This cost should be factored into any evaluation of a cloud provider’s pricing structure.

On the other hand, a cloud strategy can cut maintenance costs by having an outside resource monitor, patch and maintain the infrastructure. It can also boost levels of efficiency as multiple virtual servers can be provisioned on the same physical hardware. This often results in reduced use of datacenter space, and therefore a reduction in the demand for power and cooling.

**Which Applications Fit — and Which Don’t**

In addition to understanding the general principles associated with cloud-based application provisioning, IT managers should consider the suitability of specific types of applications for the cloud.

**Software Development, Testing and Quality Assurance**

Entities with active internal software development teams can benefit substantially from the cloud. Developers and quality assurance testers often need significant computing capacity for relatively short periods of time. Internal IT operations teams may not be able to provide this capacity quickly or cost-efficiently, which can delay important development projects and consume developers’ time.

The cloud offers developers near-immediate and relatively inexpensive access to the computing capacity they need. It can also give them access to the different environments they may need to thoroughly test how well their code runs under a variety of potential real-world conditions. This can help accelerate the delivery of new high-quality applications and services.

Just as important, with the cloud, this capacity can be rented only for as long as it is needed. This eliminates the waste associated with buying extra hardware for development teams.

**Collaboration Apps**

Email, web conferencing, document sharing and other social/collaborative applications are increasingly important to organizations seeking to increase productivity, accelerate business processes, improve decision-making, foster innovation and leverage institutional knowledge.

Cloud computing allows organizations to provide communication and collaboration tools from anywhere. This offers the ability to support work from any location, at any time and on any device. Furthermore, it provides credence to the bring-your-own-device (BYOD) phenomenon and the resulting incremental productivity offered to the organization.

Added security comes in the way of authentication and security protocols offered by the cloud service provider for access outside of the firewall. The CSP also provides ongoing maintenance efforts needed to keep protocols secure and data compliant.

**Personal Productivity Apps**

Desktop word processing, spreadsheet and presentation apps — in particular Microsoft Word, Microsoft Excel and Microsoft PowerPoint — have become staples of knowledge worker productivity. They have also become more expensive to own and manage as users increasingly work on multiple devices from diverse locations. Licensing can be a particularly thorny issue as many employees work from a varying number of devices.

Microsoft has responded to the changing needs of knowledge workers with Microsoft Office 365, a cloud-based version of the company’s popular Office suite that provides anytime/anywhere access — along with other useful features such as calendar syncing and collaboration tools. By migrating users to this type of solution, companies can reduce their software ownership costs while better supporting today’s workers.

**Big Data, Analytics and Other Computing-Intensive Apps**

Every minute of every day, users and computing endpoints generate a wealth of data. From Facebook posts to utility meter readings, this data offers tremendous potential for actionable insights about changing market dynamics, sales opportunities, operational problems and exposure to risks.
To realize this potential, companies must be able to rapidly process massive volumes of Big Data, perform sophisticated analysis of it and deliver results to users in a visually intuitive way. That kind of computing requires a lot of processing power, storage and throughput, which can be expensive to acquire and maintain. Plus, Big Data workloads are often highly sporadic, requiring massive capacity for short periods of time and then extended periods of inactivity.

Here again, the cloud is an obvious fit. With the right cloud service, organizations can get access to the Big Data processing capacity they need for as long as they need it — without massive capital expenses for capacity they don’t need. Many cloud providers also specialize in analytic applications and offer advanced and highly customizable analytic algorithms that help find the high-value “needles” in Big Data “haystacks.”

One major caveat: Organizations should seriously consider cost and time factors when moving large amounts of data to a cloud service provider’s environment. Additionally, significant costs may be incurred if data has to be moved out of that environment. However, in most cases, the capital savings and elastic scalability of cloud environments more than offset these costs.

**Disaster Recovery, Business Continuity and Records Retention**

As organizations become increasingly dependent on applications and other IT services on a moment-to-moment basis, they also must safeguard those applications and services from all types of disasters — including extreme weather, regional power outages, terrorist attacks and even a large-scale failure of an enterprise data center.

The cloud can clearly play a central role in provisioning recovery and continuity. With the cloud, replicated versions of critical applications and their associated data can be maintained in one or more locations sufficiently distant from a main enterprise data center that they are unlikely to be vulnerable to the same disaster. Users can then access those resources from other locations.

Organizations can also leverage cloud service providers to comply with regulations that govern records retention. The cloud can provide economies of scale that reduce overall storage costs — while also providing rapid access to data over the network when necessary.

**Apps That May Not Work: ERP and Other Core Systems of Record**

Most organizations have a set of core applications, such as enterprise resource planning (ERP) systems, that function as their primary systems of record. It may be challenging or impractical to migrate these applications to the cloud for a variety of reasons:

- **Performance issues:** Because these applications tend to be transaction-intensive, they may require high network throughput and very low latency. This performance may be difficult to achieve in a cloud environment.

- **High-availability requirements:** While the cloud offers excellent overall continuity and availability, any application accessed over the Internet is susceptible to the occasional “hiccup.” For systems where even a relatively brief interruption can have significant consequences, organizations may be better off investing in high-availability infrastructure in an in-house data center.

- **Sensitive data:** Systems of record are almost always repositories for some of an organization’s most sensitive information — including customer data and financial records. Regulatory compliance and governance best practices may therefore prevent movement of this data to the cloud.

- **Application architecture:** For companies that have been running their businesses on the same ERP system for many years, the architecture of the application itself may preclude migration to a virtual environment.

The cloud is not a panacea. It won’t eliminate every IT challenge an organization faces, and it isn’t appropriate for every application. But with the right insight and the right partners, companies can leverage the evolving range of cloud solutions to drive down costs, improve productivity, empower managers to make better decisions and drive the kind of innovation that dramatically improves business performance in dynamic and competitive markets.

---

**The Best of Both Worlds: Leveraging the Hybrid Cloud**

To move some applications to the cloud, organizations may be best served by adopting a hybrid model, which combines multiple types of cloud or conventional infrastructure. Hybrid-cloud models include:

- **Own the base, rent the spike:** Under this model, normal day-to-day workloads run on in-house IT infrastructure (which can be either conventional or a private cloud). Off-premises hosted-cloud resources are used only during periods of peak demand to maintain service levels to users.

- **Cloud as firewall:** Under this model, an off-premises cloud environment is used to run customer-facing processes that may support web or mobile applications. Back-end application components such as databases and transaction processing systems remain in-house.

- **Compliance segmentation:** Here, data is split between in-house and off-premises environments. This enables compliance with data-related regulatory mandates, while still allowing the benefits of cloud computing to be applied where appropriate.
Your organization has successfully migrated data and applications to the cloud. Along with the many benefits of cloud adoption, the enterprise now must address cloud computing security issues. In today's threat-filled cyber environment, keeping pace with cloud computing security isn't just a luxury; it's a necessity.

This kind of threat prevention includes a series of strategies that builds a multilayer security protection plan designed to prevent malicious attacks from entering your cloud environment and corrupting applications, systems and data.

To help maintain cloud security, CDW offers a dedicated team of security experts, including dozens of solution architects committed to designing custom cloud architectures, cloud strategies, services and solutions.

We also have advanced cloud specialists to assist with implementation and long-term management solutions. And our cloud portfolio includes more than 200 products spanning 36 categories.

CDW can help with the entire cloud-computing lifecycle, from selecting which cloud models are best for an organization to simplifying the challenging process of moving applications and data from the existing infrastructure to the cloud.

Our approach includes:

- An initial discovery session to understand your goals, requirements and budget
- An assessment review of your existing environment and definition of project requirements
- Detailed manufacturer evaluations, recommendations, future-environment design and proof of concept
- Procurement, configuration and deployment of the final solution
- Telephone support and product lifecycle support

CDW account managers and solution architects are ready to assist with every phase of choosing and leveraging the right solutions for your cloud needs.

Adobe Creative Cloud for teams has all the tools that you love, totally re-imagined. Enhancing creativity with cloud storage, one-stop publishing, expert training and support, flexible license management, hassle-free compliance and lower costs. Creative Cloud for teams lets you maximize your budget and leverage centralized administrative tools that make it easy for IT to purchase, deploy and manage Creative Cloud along with the changing needs of your team.

CDW.com/adobe

To learn more about CDW's cloud computing solutions, contact your CDW account manager, call 800.800.4239 or visit CDW.com/cloud