



IBM

IBM Cloud

# Cloud Managed Services: A comparison guide

What to look for when choosing  
your cloud provider

Why a managed cloud?	3
What should you look for in a cloud managed services provider?	4
<b>CHOICE:</b> What are your options?	5
<b>SECURITY:</b> Can your provider really protect your data and applications?	9
<b>MANAGEMENT:</b> What can the provider actually do for you?	13
<b>GLOBAL PRESENCE:</b> Does your provider deliver where – and how – you need it to?	17
Where competitors fall short, IBM can deliver	20
IBM understands the beginning, transition and destination in your journey to the cloud	21
How does your prospective cloud managed services provider answer these questions?	22
Take the next step	23

# Why a managed cloud?

Enterprises are turning to the cloud to deliver compelling customer experiences, power innovative business models and achieve business agility. They're looking to move critical workloads to a secure, reliable cloud infrastructure, and integrate existing systems of record with dynamic new mobile and social applications. That's not easy, so many enterprises partner with a provider to deploy and manage the cloud for them.

## Using managed cloud to best advantage

By adopting cloud managed services, the enterprise can better support key business activities:

**Match the environment to the workload** – Deploy multiple infrastructures appropriate for specific workloads, like CRM, ERP or financials

**Optimize the application lifecycle** – Set up one infrastructure for initial application proof-of-concept and dev/test, and another for production, each configured for best results

**Split applications** – Allocate infrastructure tuned for different application components, such as a web application front end and a database back end

**Rapid scaling** – Our highly configurable platform enables you to right size your server environment from day one and scale as required. With enterprise-class features such as rapid service activation and deactivation; infrastructure monitoring and reporting; and security and patch management, our managed cloud solution is designed so that you can focus on continuous innovation while we take care of the infrastructure.

## The right cloud managed services provider can offer:

- Access to the best infrastructure without added CAPEX
- Greater business agility through freedom of choice
- Guaranteed service levels with consistent performance
- Enhanced security with global delivery if required
- Less risk and cost with usage-based pricing
- Relief for over-burdened IT staff so they can focus on higher-value work

## Which workloads are best for a managed cloud?

- Enterprise-grade workloads of all shapes and sizes are a good match for managed cloud services. The ideal fit is workloads that scale up and down periodically, requiring extra capacity from the cloud, and any application that requires integration between the cloud and on-premises systems.

## Enterprise applications

- Critical back-office applications such as ERP, CRM, SAP, Oracle or home-grown applications – the applications that were not written for cloud
- Line-of-business and departmental applications
- Core industry-specific applications

## Enterprise workloads across the application lifecycle

- Dev/test
- Load test
- Quality assurance
- Pre-production
- Training and staging environments

“A full **91%** of enterprises seek cloud implementation assistance, with 13% of those turning to a managed services provider.”

– Frost & Sullivan, *Cloud Based Managed Services: Tips for Selecting a Provider that Can Help You Re-Tool Your IT Department*<sup>1</sup>

# What should you look for in a cloud managed services provider?

**A managed cloud provider should meet *all* of your needs, not just some.**

**Choice** – Choice of infrastructure, location, services and delivery, with coverage for the operating systems and hardware that run your business critical applications

**Security** – The high levels of security required for your business, with an understanding of the division of responsibility between you and the provider

**Management** – The skills for end-to-end management of the cloud – infrastructure, platform-as-a-service and application support

**Global presence** – Housing data and applications where regulations and business requirements dictate

Choosing the right provider to deploy and manage your cloud is not a simple business decision. Gaps in security, services, technology, expertise and ability to deliver could have serious consequences.

The characteristics of an expert cloud managed services provider

**Core expertise in infrastructure, workload, application management and professional services** – Look for a provider able to understand your business needs, suggest the best solutions, and then execute in a way that ensures success.

**Support for multiple hardware types and hypervisors** – Pay attention to whether the provider can match the workload to the infrastructure that can best support it.

**Hybrid management expertise** – The provider should be able to split workloads and data among different physical and virtual environments to provide the best cost and performance benefits.

**Customizable services and SLAs** – Seek alignment with your business goals, through guarantees of specific service parameters and the ability to tailor services according to your needs.

**Robust security** – Look for security expertise and capabilities that are equal to or exceed what you can do on your own, to ensure that workloads and data remain accessible at all times.

**Compliance assurance and related reporting** – Check to see if the provider can prove compliance, and whether it has comprehensive reporting capabilities that can meet regulatory requirements.

**Robust portfolio of managed services** – Look beyond the basic cloud managed services offering for added value – assistance with tasks such as environment configuration, governance, and management of specialized workloads such as ERP or CRM.

## CHOICE:

# What are your options?

---

“The right provider offers not only applications and infrastructure, but the expertise to augment your staff and to manage resources to meet your business’s needs and goals.”


– Frost & Sullivan, *Cloud Based Managed Services: Tips for Selecting a Provider that Can Help You Re-Tool Your IT Department* <sup>2</sup>

---

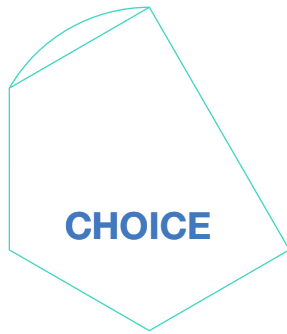
Not all clouds are created equal, and neither are cloud providers. A cloud managed services provider should be flexible, offering you choices – of hardware, operating system and platform components – to align your cloud deployment with your business and workload requirements.

### **Why can’t all providers deliver the choices you need?**

Some providers offer a one-size-fits-all infrastructure that may not necessarily allow you to achieve optimal price-performance, leverage your existing skills and resources, or guarantee high SLAs as you deploy business-critical applications and data to the cloud. Often, they offer only off-premises, virtualized public cloud infrastructure that brings with it concerns over price-performance, control and security.



Choice of infrastructure, location, services and delivery, with coverage for the operating systems and hardware that run your business critical applications



Infrastructure, geographic location,  
services, delivery, operating  
systems and hardware

## “How quickly can you get me up and running?”

Rapid provisioning to support DevOps and quickly roll out new business models and innovative applications is one of the primary reasons to move to the cloud. It’s about seizing competitive advantage. Many providers deliver infrastructure only – virtual CPUs, storage and networking. It’s up to you, or a third party, to configure and manage it, and that can slow your enterprise down.

### Look for fully provisioned environments, ready to go

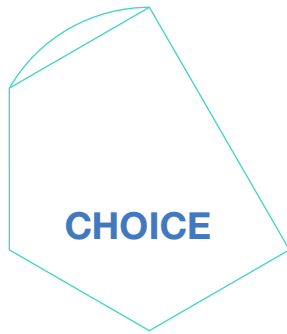
A provider worthy of consideration uses self-service capabilities and automation to quickly provision hosted cloud environments, helping you achieve DevOps productivity and speed time-to-market. Operating systems should be patched to current levels, middleware installed, the virtual machines fully configured, tested and verified so that they’re ready for immediate use.

## “What are my choices for hardware and operating systems?”

When migrating to the cloud, it’s best to align workload characteristics with the infrastructure to optimize performance. The closer the match to your existing infrastructure, the less complex the task becomes – and that means less risk, lower costs, greater agility and faster time-to-market.

### Look for operating environments that align with *your* needs, not the provider’s

A provider should be able to support a wide range of operating environments so that the cloud dovetails with your existing environment and skill set – Red Hat Enterprise Linux on x86, Microsoft Windows on x86, or proprietary operating systems like IBM AIX on IBM Power Systems. In addition, the vendor should allow you to precisely match infrastructure and platform services to our workload needs, rather than fixed-size deployments. That lets you deploy on the infrastructure best able to meet your business objectives.



Infrastructure, geographic location,  
services, delivery, operating  
systems and hardware

### “Can you meet service levels?”

Many enterprises have yet to implement a cloud strategy because they lack confidence that the cloud can reliably deliver the performance and service levels they need. The issue is not just infrastructure – the operating system that runs on top of it must also meet service level requirements, yet some providers will only provide SLAs for servers, storage and/or networking. That increases your business risk, because responsibility is put back on your shoulders.

#### **Look for SLAs that cover the entire managed cloud environment**

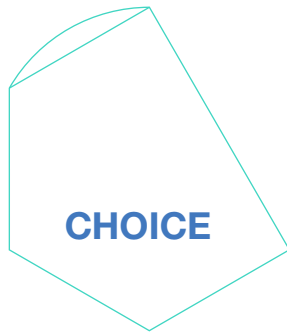
Different workloads have different Service Level Agreement requirements, and your provider should be able to deliver the right level at the right price, with SLAs based on workload characteristics. SLAs should span IaaS and PaaS, extending all the way up to the operating system level.

### “Can you deliver a consistent experience across my business?”

To meet customer and business expectations, it's important to have the same infrastructure, software, processes and managed services in place. This is particularly important in a disaster recovery, workload migration or global enterprise scenario. Consistency helps assure SLAs are met and can help minimize the risk of potential technical and performance issues.

#### **IBM delivers a consistent infrastructure, set of management practices, and delivery team - worldwide**

IBM data centers hardware and software is constantly updated so you are not forced to use backlevel or unpatched infrastructure. The architecture and functionality is uniform, local or global – standardized deployments and service delivery that can reduce risk and complexity.



Infrastructure, geographic location,  
services, delivery, operating  
systems and hardware

### “Can I mix public and private clouds?”

Deployment choices let you select the cloud that best matches your workload and business requirements – a public cloud for cost-effective, rapid scalability or a private cloud for greater security capabilities with consistent management that can simplify DevOps for greater business agility.

#### **Look for a cloud portfolio that delivers both choice and consistency**

A managed cloud provider should enable you to deploy different parts of your enterprise workloads – such as various SAP modules – where they make the most sense based on security, scalability and SLA requirements. That means public or private clouds, all from the same provider. Management should be simple and streamlined, so that you gain business agility that helps you respond to new customer demands and competitive threats.

### “How well qualified are you to meet my needs?”

Cloud managed services should not limit your options, yet many providers do by depending on third parties. That can add complexity and risk to the relationship and may open up service and skill gaps. Looking at total expertise and the ability to deliver a full range of services can help accelerate business results.

#### **Look for a single provider able to help meet your needs from end to end**

A provider should have the full range of required knowledge, service portfolio, skills and experience in-house. Seek one relationship with a single partner able to add value to the cloud, with professional services that include migration and strategy, a choice of delivery models, and support for options such as use of your own hardware.



## SECURITY:

# Can your provider really protect your data and applications?

---

“Today, the majority of CxOs, irrespective of role, think IT security is a top risk.”


– IBM Institute for Business Value, *Redefining Boundaries: Insights from the Global C-suite Study*.<sup>3</sup>

---

When you lack good security, you run significant risks – valued clients leaving because of security breaches, losing the trust of potential customers, damage to your reputation in your industry, and potential penalties from regulators. That’s why a cloud provider should treat client data as if it were their own. The cloud should be built from the ground up with security as part of the design, not a retrofitted set of “fixes” applied as an afterthought in response to breaches.

### **Why can’t all providers deliver adequate security?**

Providers may claim that their clouds are very secure, but gaps in infrastructure, services and physical security could leave you vulnerable. Some providers fill these gaps by using security services delivered by third parties – which can increase risk exposure. I have to think clients also have certain responsibilities to help keep their data and applications safe even if on the Cloud. Security options are sometimes provided by third parties, which can increase risk exposure. What’s needed is multiple layers of security from the provider itself – a full range of managed security services built in, the ability to help clients meet their compliance and data residency needs, and additional services that strengthen reporting and vulnerability protection.



The high levels of security required for compliance, with appropriate division of responsibility between you and the provider



## “Where is my data, exactly?”

Not all providers can house your data where you expect it to be. You may know nothing about the security and risk exposure of the data center where your data and applications are actually housed. And data sovereignty requirements might require you to store data in a particular location – something you may not be able to meet without the assurance that your data is where you placed it.

### Look for control of your infrastructure and data

A provider should keep your data in the same city where you agree it should be placed. The provider should also have a data center network extensive enough to house data on its own infrastructure where it claims to do business, rather than having to turn to third parties. In addition, it should have secure disaster recovery sites so that you know where your data goes in the event of an outage.

## “Who’s responsible for security?”

Maintaining security is a never-ending task, from monitoring and prevention of attacks to applying security patches, hardening infrastructure and managing access. Not all providers can take responsibility for all that needs to be done. When working with a potential vendor, understanding what level of security compliance they provide – and how much work they do to prove that compliance, is important. Where does the division of responsibility begin and end? For some providers, once they have provided you with the server hardware – the overall responsibility for workload security and compliance rests with you.

### Look at how the provider manages their own security

The provider should provide security for client cloud deployments using the same tools, standards and methods that protect its own systems. It should also be able to take full responsibility for everything or any subset of things that are part of the managed cloud rather than leave it to you or a third party. Provider and client security responsibilities should be clearly defined so there are no gaps.



Appropriate division of  
responsibility between you  
and the provider

### “How do I know your security is adequate?”

Simply claiming that a cloud is secure and can help you meet your compliance obligations isn't enough. Since you're responsible for compliance with regulatory mandates, your provider should have capabilities that help you meet applicable standards. Some may show many certifications, but look closer and you may find that coverage is only for select services and/or locations. Ongoing security should include regular vulnerability scanning that covers the entire infrastructure – both hardware and software – as well as policies and procedures.

#### Look for quality in security and compliance

Look for certification to ISO 27001 and 27018 standards. Check that your vendor can provide an environment that helps you meet your compliance requirements for PCI Standards (PCI-DSS) and the Health Insurance Portability and Accountability Act (HIPAA). All certifications and security measures should be validated annually by external auditors with evidence demonstrated through AICPA Service Organization Control (SOC) level 1 and 2 reporting.

### “How extensive are your security measures?”

Security threats can come from any direction – over the network, from malware, unauthorized access, software exploits, even physical theft. Any gap in security can leave your enterprise vulnerable. Not all cloud providers are able to offer comprehensive capabilities to help protect your cloud, your data – and your applications – which puts the security burden on you.

#### Look for security in depth

A provider should build in multiple layers of security, from the data center all the way through to the operating system. Clouds should be hosted in Tier-3 – or equivalent – data centers with best-of-breed physical security. Server instances and storage should be segregated to isolate your data, and backup media should be encrypted in case of loss. Security should also cover the OS, database and middleware as part of the service, with vulnerability management provided for the managed environment.



Appropriate division of  
responsibility between you  
and the provider

### “What if something goes wrong?”

Failure to recover promptly from a disaster can have dramatic, long-lasting impacts on your enterprise. There’s more than lost revenue and productivity at stake; customer confidence can be irreversibly damaged by a poorly handled outage.

#### Look for backup and recovery that is not an afterthought

A provider should be able to deliver alternate-site disaster recovery and help you get back online quickly, with production-level SLAs that remain in effect during the disaster. That capability should also be tested regularly, and disaster recovery consulting should be provided to ensure that you have a reliable, optimized plan in place.

### “How much experience do you have in IT security?”

Security is a very complex, systemic issue where experience matters, because not all providers have had to deal with threats that extend beyond their own, limited set of services and competencies. It’s important that the provider has seen, and successfully managed, a broad range of security issues.

#### Look for experience in enterprise computing

A provider should have security controls that meet or exceed industry best practices at the management layer, with the same standard security policies applied to all clients. Ask about the vendor’s track record of delivering reliable, resilient, IT services with robust security capabilities— proven success in traditional enterprise IT and cloud security can help give you peace of mind that your cloud will be equally well protected

## MANAGEMENT:

# What can the provider actually do for you?

---

“According to Frost & Sullivan, enterprises that manage their own cloud environments spend three to five dollars for every dollar they spend on IaaS.”

– Frost & Sullivan, *Avoid Budget Overruns: A Guide to Assessing Cloud IT Economics* <sup>4</sup>

---

Managing cloud deployments, applications and data can be very complex, introducing different tools, processes, management interfaces and skill requirements. That can drive up costs and have a real impact on service levels, business agility and customer experiences. For this reason, many IT leaders hesitate to bring highly customized, far-reaching systems like SAP into the cloud – the risks of failure can seem too high. The right cloud managed services provider can help overcome these barriers, enabling cloud-related efficiencies to be introduced to enterprise workloads.

### **Why can't all providers deliver a fully managed cloud solution?**

The fact is that deploying and managing an enterprise cloud extends beyond the IaaS offerings that many cloud providers deliver. Many lack depth outside their own portfolio and may not be able to manage the cloud above the hardware level, up through the middleware and database. They'll either leave management to you, or bring in third parties to fill service and expertise gaps. Standardization may also be a challenge: providers may lack IT Infrastructure Library (ITIL)-based practices that enable consistent and efficient service management designed for business-critical applications.





end-to-end management,  
infrastructure, platform-as-a-service  
and application support

### “Can you manage the whole cloud stack for me, both IaaS and PaaS?”

One of the reasons enterprises partner with a cloud managed services provider is to ease the burden of management – the cost, complexity, risk and impact on productivity and service levels. But some vendors only get you partway there, with services that do not span both the infrastructure and the platform that runs on top of it. They may rely on third parties or not offer the services you need at all.

#### Look for an environment managed from end to end

If you have a provider you should be able to cover everything from the infrastructure to the operating system, middleware and databases, and even the application environment. Your staff should not have to focus on day-to-day management, so they can spend time working on higher-value projects that can drive innovation and competitive advantage.

### “How robust are your management practices?”

Comprehensive, best-practice management of the cloud infrastructure and platform that sits on top of it can improve productivity and helps ensure higher service levels by reducing the workload on your IT staff. That can enable you to reliably meet customer expectations and achieve business objectives for service delivery and cost.

#### Look for consistent management according to recognized standards

The provider should use a common management platform that brings together business, IT and operational support for uniform end-to-end management. All management processes should be ITIL compliant, ensuring that current industry best practices are followed. That means consistency and repeatability, with a high degree of automation that can improve efficiency and effectiveness.



end-to-end management,  
infrastructure, platform-as-a-service  
and application support

### “Can you simplify tasks for my IT staff?”

Even with a fully managed cloud, IT staff must perform procedures such as provisioning and configuration. Multiple management interfaces, processes and skill sets add to complexity and cost, and can bring down productivity. It becomes more difficult to access cloud resources and accomplish the tasks that your staff is responsible for – when it should be simpler.

#### Look for streamlined, automated cloud management

The vendor should provide a simple self-service interface that enables rapid access to the managed environment and all services. With such an interface, staff can select hardware, CPU, memory and storage, along with service level, operating system and optional services such as application monitoring. This ability to leverage automation and unified management tools can speed time-to-market and enhance DevOps productivity.

### “Can you fully support my enterprise applications?”

Enterprises are gaining significant business value by cloud-enabling enterprise applications such as SAP and Oracle, along with their data. But that creates a new challenge for IT: managing and securing a cloud deployment alongside the core IT infrastructure, along with the applications and databases. Some cloud providers struggle to provide full support for these environments.

#### Look for dedicated support for leading enterprise applications

For users of these enterprise applications, the vendor should offer managed as-a-service support that encompasses the entire enterprise platform. A vendor that can manage up the stack, including core infrastructure and enterprise platform components such as the SAP Basis and database layers, business-centric SLAs for enterprise applications including SAP, SAP HANA and Oracle will be better able to help maintain service level commitments.



end-to-end management,  
infrastructure, platform-as-a-service  
and application support

### “Can you assist me in migrating my cloud-enabled workloads to your environment?”

“Lifting and shifting” key enterprise workloads to a cloud environment is often required to quickly and efficiently address business needs. However, the move can be a complicated process that impacts your productivity, consuming valuable IT resources. If your provider does not support your choice of operating system, it may not be possible at all.

#### Look for the ability to ease transition to the cloud

The provider should offer dedicated services that utilize standardized, repeatable processes and automation to simplifying the move and reduce migration costs compared to re-installing applications. The provider should also allow you to maintain your existing application configuration, and not force expensive, time-consuming upgrades of customized applications such as SAP.

### “Can I choose what I want you to manage for me?”

While a provider should offer a robust set of managed services that extend from basic infrastructure up through the platform that runs on it, you should not be forced to accept services you neither want nor need. It may be preferable, for internal compliance, security or organizational reasons, to keep some management activities and responsibilities in the hands of your IT staff.

#### Look for flexibility in management

The provider should give you choices in how you manage your cloud environment, offering a full set of services but allowing you to take on management tasks to the greatest degree possible if that is your requirement. Look for multiple levels of service, up to and including unmanaged infrastructure. That lets you match the service you receive to your individual business needs.




## GLOBAL PRESENCE:

# Does your provider deliver where – and how – you need it to?

Globalization has created new challenges for enterprises. Those that operate around the world need consistency in service, support and cloud environments everywhere, but they face major variations in regulation and the ability of cloud providers to deliver a uniform set of services. The issues they face may differ from region to region, but their cloud environments should not.

### **Why can't all providers consistently deliver on a global level?**

Some providers focus their efforts on one region. Others aspire to be global, but must rely on third party data center providers. Few can deliver a standardized cost-efficient, cloud with robust security on a global scale, which is a critical consideration for multinational enterprises. Those that choose these providers may be forced into adopting a patchwork of varying cloud environments and vendor relationships – a source of increased compliance and security risk, along with cost.



Housing data and  
applications where  
regulations and business  
requirements dictate



data and applications where  
regulations and business  
requirements dictate

### “Regulations require me to house my data in a specific region. Do you have a data center there?”

Data sovereignty mandates often require data to be placed where business is done. That makes point of presence a critical selection criterion for global enterprises. A cloud provider that does not have a data center where the client needs it might have to bring in a third party whose infrastructure and support capacity doesn't align with business needs. That can potentially add to security concerns and potentially impact critical SLAs.

#### Look for a global data center network

The provider should have data centers owned and operated by its own staff in the locations you require. And in those cases where specific requirements demand hosting in a location that the provider does not serve, a rigorous approval methodology should be in place to help ensure that the data center you do use meets your standards for infrastructure, SLA, cost and security.

### “Are your data centers and management services all the same?”

Global enterprises need to deliver a consistent experience to their business and their customers regardless of location. Borders should not matter; the enterprise should appear the same everywhere. If a cloud provider cannot deliver the same environment, management service, standards and delivery methods everywhere, it can be difficult to achieve that consistency.

#### Look for the same cloud experience, everywhere

The provider should deliver the cloud you contract for, whether it's in Asia, North America or anywhere else. Look for a consistent, one-team, one-practice approach with standardized services, management and infrastructure that helps to ensure uniform delivery and service levels worldwide.



data and applications where regulations and business requirements dictate

### “What if I need to move data from one data center to another?”

Transporting large volumes of data from one location to another can significantly increase costs with some providers. It also can expose that data to increased risk of interception, if the provider must use the Internet. That can inhibit business agility, because there may be strong financial and security incentives to not move data even if there’s a good business reason to do so.

#### Look for a provider with its own global network

A provider should have a private global network connecting all its data centers. Selecting such a provider can give you greater agility as you respond to shifting marketplace, business and regulatory needs. A secure private network can also enhance disaster recovery by allowing rapid restoration from an alternate site.

### “What if your data center partner goes out of business?”

Reliance on third parties to build out a global data center network adds a new risk factor: the cloud provider may not be able to control the reliability of the third party, nor be willing to assume liability for protection of your data.

#### Look for a provider able to house your data in its own data centers

A provider that owns and operates a global network of data centers need not rely on third parties. Know who is providing the infrastructure’s availability and safeguarding your data. Also look to see that your data will not be shifted from its specified location, unless you ask for it to be moved.

# Where competitors fall short, IBM can deliver

IBM Cloud Managed Services is a production-ready cloud environment built for enterprise-class performance, combining a robust IaaS solution with a full set of managed services. It's a "fit-for-purpose" on- or off-premises answer for enterprise cloud needs, delivering:

**A wide choice of compute, storage and network configurations** that are highly flexible, scalable and available, supporting Linux, Windows and IBM AIX and multiple database and middleware options

**Best-practice security** with vulnerability scanning and protection from physical intrusion

**Disaster recovery** on a global scale with failover and fallback

**Compliance services** that meet the most rigorous standards for privacy and protection

**Solutions for SAP, SAP HANA and Oracle** along with other ERP and CRM workloads, so you can cloud-enable your own applications

## IBM Cloud Managed Services: Cloud from end to end

- Integrated managed services for infrastructure, change management, configuration, security monitoring and patching, asset management and OS patching
- One consistent, easy-to-use self-service management portal
- Fully managed high-availability, backup and disaster recovery solutions
- Managed database and middleware
- Wide range of deployment options – your site, an IBM data center, approved third-party, shared or dedicated
- Application management services for ERP workloads
- Choice of SLAs, up to the application level

# IBM understands the beginning, transition and destination in your journey to the cloud

A fundamental reason why enterprises like yours turn to cloud managed services is for help in transitioning to the cloud. IBM Cloud Managed Services builds on IBM's long experience in cloud, enterprise computing, security and business transformation to help make that journey smoother and quicker. IBM is a partner that can help you control your journey to cloud – from beginning to end – with knowledge of both on premises and cloud deployments, legacy and “born on the cloud” applications – plus proven expertise in planning, transition, migration and change management.

## **IBM understands that moving to the cloud is a journey that goes beyond managed infrastructure:**

- Assessing and selecting applications suitable for the cloud
- Planning and preparing applications to move
- Migrating applications and data to the cloud
- Managing cloud infrastructure
- Managing applications in the cloud
- Continuous optimization of the cloud

Compare IBM to other providers. You'll find that their solutions have multiple moving parts. Some may require multiple, specialized partners to cover all the services needed to migrate enterprise-grade workloads to the cloud – and once there, deliver managed services and the added expertise needed to help you achieve your business objectives.

# How does your prospective cloud managed services provider answer these questions?

Tough questions about:	
<h2>Choice</h2> <p>What's your <b>track record</b> in mission-critical enterprise computing?</p> <p>Can you support my <b>choice of technology</b> and deployment model?</p> <p>Can you deliver <b>everything I need</b> – infrastructure, platform and managed services?</p>	
<h2>Security</h2> <p>Is your physical and IT <b>security</b> up to my standards?</p> <p>Where does your <b>responsibility</b> for security and service levels end – and mine begin?</p> <p>How good are your <b>disaster recovery</b> capabilities?</p>	
<h2>Management</h2> <p>When you say you manage my environment – exactly <b>what are you managing</b>?</p> <p>Am I dealing with <b>one company or several</b>?</p> <p>How good – and how extensive – is your <b>enterprise application support</b>?</p> <p>Do you provide <b>flexibility</b> in management? Can I choose which tasks I manage and which I want you to take on?</p>	
<h2>Global Presence</h2> <p>Can you meet my needs on a <b>global scale</b>?</p> <p>Can you place my data and workloads <b>where I need them</b>?</p> <p>Do you require the <b>assistance of third parties</b> to achieve coverage where I need it?</p>	

# Take the next step.

## Find out more about IBM Cloud Managed Services

**Visit the IBM Cloud Managed Services >**

<https://www.ibm.com/cloud-computing/infrastructure/managed-cloud-hosting>

**Request an IBM Cloud Affinity Analysis >**

Understand which workloads are optimal so you can demonstrate early success in your cloud adoption. Let our experts help you. The IBM Cloud Affinity Analysis is a low-cost, face-to-face assessment that provides a qualitative analysis of each designated workload, including its overall affinity to cloud, the pain versus gain of moving it to cloud, and whether it's better suited for public, private or a managed hosted environment.



© Copyright IBM Corporation 2016

IBM Corporation  
New Orchard Road  
Armonk, NY 10504

Produced in the United States of America  
June 2016

IBM, the IBM logo, ibm.com, Bluemix, IBM Cloud Managed Services, IBM UrbanCode, IBM Watson, IBM z Systems and POWER are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml)

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions. It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation. Statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

<sup>1</sup>*Cloud Based Managed Services: Tips for Selecting a Provider that Can Help You Re-Tool Your IT Department.* Frost & Sullivan. June 2016.

<sup>2</sup>Ibid.

<sup>3</sup>*Redefining Boundaries: Insights from the Global C-suite Study.* IBM Institute for Business Value. November 2015.

<sup>4</sup>*Avoid Budget Overruns: A Guide to Assessing Cloud IT Economics.* Frost & Sullivan. June 2016.



Please recycle