Cloud Managed Services: A comparison guide

What to look for when choosing your cloud provider

IBM

Which workloads are best for a managed cloud?

Enterprise-grade workloads of all shapes and sizes are a good match for managed cloud services. More and more, that means leading ERP platforms like SAP, as part of a digital transformation strategy. 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

- Legacy back-office applications not originally developed for the cloud, such as ERP, CRM, SAP, Oracle or home-grown line-of-business applications
- Core industry-specific applications

Enterprise workloads across the application lifecycle

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

Why a managed cloud?

Increasingly, enterprises are cloud-enabling enterprise applications like SAP to power innovative business models and achieve business agility. They're looking to move critical workloads and data 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 partner with a provider to deploy and manage the cloud and their enterprise applications for them.

The right cloud managed services provider can offer:

- Advice and assistance when migrating to the cloud
- Access to the best infrastructure without added CAPEX
- Greater business agility through multiple levels of management options
- Guaranteed service levels with consistent application performance
- Enhanced security with global delivery if required
- Less risk and cost with usage-based pricing that avoids over-provisioning
- Deployment and management of critical enterprise workloads and data

SAP S/4HANA adoption: The value of a managed cloud

It's been made clear that SAP's S/4HANA next-generation business suite is the future and many enterprises are looking to combine adoption of the new platform with a move to the cloud.

The challenge is that since S/4HANA is relatively new, it can be difficult to find people with the skills to run the platform effectively, and the move can put stress on limited IT resources. A well-qualified managed services provider can help reduce those issues in several ways:

- Acceleration of SAP module adoption and migration to speed time-to-value
- Optimization of the ERP environment to improve performance, service levels and cost
- Dedicated management of the S/4HANA suite

Agility to capture the value of Artificial Intelligence (AI) computing

Research conducted in 2017 by Frost & Sullivan found that 70 percent of IT leaders are looking to expand the capabilities of their IT landscape by integrating AI technology.

Their goal is innovation: using data in new ways to deliver differentiating experiences, whether it's analyzing unstructured customer interaction data to generate deeper insight, leveraging weather data to make real-time business decisions or opening up new revenue streams by empowering clients. Providers should facilitate innovations like these, through AI APIs that enable the rapid creation of new applications. There are two key considerations:

- **Business agility vs. infrastructure investment** – Dynamic scalability is essential for AI workloads, which makes them ideal for cloud deployment. But at the same time, innovation can cause business models to change rapidly and often, making investment in dedicated cloud infrastructure risky

- **IT and innovation resource limits** – The management demands of a cloud infrastructure puts a heavy load on IT staff, whose talents would be better applied to driving innovation.

Together, these issues make a powerful case for cloud managed services – and partnering with a provider that fully understands the potential and demands of AI computing.

How does a managed cloud add business value?

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 and 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

Scale rapidly – 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.

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 compliance, with appropriate division of responsibility between you and the provider

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

Expertise – Understanding not just the cloud itself, but the workloads running on it

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

What should you look for?

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 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 demonstrate that its capabilities meet compliance standards, and whether its reporting capabilities can help you meet regulatory requirements.

Robust portfolio of managed services – Look beyond the basic offering for added value–assistance with tasks such as workload selection and migration, environment configuration, governance, and management of specialized workloads such as SAP.

Assistance moving to the cloud – Look for a provider that can help you determine the right workloads to move to cloud, help you integrate legacy apps with those you are moving to cloud and provide both pre-migration and migration services.

Choice

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

> "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.*[1]

What are your options?

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?
Many providers offer one-size-fits-all infrastructure that does 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

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

Questions you should ask about choices in cloud deployment

"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 slows 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.

Choice

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 networking. That increases your business risk, because responsibility is put back on your shoulders.

Look for SLAs that cover the entire managed cloud

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

“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 assures SLAs are met and minimizes the risk of potential technical, performance and compliance issues.

Look for a provider that provides consistency through one set of management practices and one delivery team worldwide

All IBM data center hardware and software is continually updated so you are not forced to use back-level or unpatched infrastructure. The architecture and functionality are uniform – standardized deployments and service delivery that reduce risk and complexity both locally and globally.

Choice

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, 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 adds 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 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 strategy development, pre-migration planning, migration services, a choice of delivery models, and support for options such as use of your own hardware.

Security

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

Can your provider really help protect your data and applications?

In a recent survey conducted by Frost & Sullivan, 76% of CIOs ranked improved security and compliance reporting for SAP or Oracle workloads as a leading benefit of managed services.[2]

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. There may also be limitations in keeping your data and applications safe because their security expertise is limited to infrastructure. Security options are sometimes provided by third parties, which increases 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 you meet compliance and data residency needs, and additional services that strengthen reporting and vulnerability protection.

Security

Appropriate division of responsibility between you and the provider

Questions you should ask about data infrastructure and security

"Where is my data, exactly?"

Not all providers can promise that your data is 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 mandate that you store data in a particular location – something you may not be able to achieve 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 have agreed 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 full 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 handle the security of everything that's part of the managed environment, rather than leave it to you or a third party. Provider and client security responsibilities should be clearly defined so there are no gaps.

Security

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, 27018 and 22301 standards. 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 comprehensively 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.

Security

Appropriate division of responsibility between you and the provider

“What if something goes wrong?”

Failure to recover promptly from a disaster can have a dramatic, long-lasting impact 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 get you 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, secure IT services – proven success in traditional enterprise IT and cloud security helps give you peace of mind that your cloud will be equally well protected.

Management

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

Choosing a managed services partner that is able to deliver on your needs is not easy. Among businesses surveyed by Frost & Sullivan, 77% cited "finding the right partner" as a top challenge to their managed services initiative.[3]

What can the provider actually do for you?

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 are just 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.

Management

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

Questions to ask about cloud management

"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

A provider 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 improves productivity and helps ensure higher service levels by reducing the workload on your IT staff. This 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 always followed. That means consistency and repeatability, with a high degree of automation that can improve efficiency and effectiveness.

Management

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 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 significantly 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 S/4HANA and Oracle will be better able to maintain service level commitments.

Management

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?”

Enterprise applications like SAP do not exist in a vacuum. They must interact with other applications “lifting and shifting” other applications in addition to core 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 be able to guide you with advisory and consulting services that help you determine which workloads are most suitable for deployment in the cloud, and plan for the transition. Dedicated migration services should utilize standardized, repeatable processes and automation to simplifying the move and reduce 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.

Expertise

Understanding not just the cloud itself, but the workloads running on it

"82% of managed services users say they consider the advice of their managed services partner to be extremely or very important."

Frost & Sullivan, *Are Cloud Managed Services Right For Your Business?: Creating a Successful Business Case*[4]

How capable is your provider?

Achieving the benefits of cloud deployment takes more than infrastructure. The nature of the workload must also be fully understood, including how it interfaces with other systems, data and applications. This is especially true of complex enterprise systems such as SAP. Achieving a smooth migration, maintaining integrity and hitting SLA targets requires deep expertise in cloud environments as well as migration, organization, governance and ongoing management.

Why can't all providers help meet strategic enterprise goals?
Many cloud vendors have focused on growing their business through infrastructure offerings. Enterprise workload migration and management capabilities have been given a lower priority. In addition, relatively few have extensive experience in enterprise-level computing. Without a solid foundation of expertise and proven methodologies to draw upon, they may not be able to address all of the challenges involved in moving core enterprise workloads to the cloud.

Expertise

Understanding not just the cloud itself, but the workloads running on it

Questions to ask about expertise

"Can you help me plan, as well as execute?"

There are many activities surrounding workload migration to the cloud, from organizational and governance changes to making sure that necessary changes are made to system interfaces and connections. Not all vendors have the expertise needed to fully comprehend the range of challenges, actions and implications that may arise when dealing with complex enterprise workloads.

Look for a vendor that fully engages with your team

A provider should forge solid relationships at every level from specialist all the way up to the CIO, and take a strategic approach to planning. Look beyond the activities associated with the migration itself, to all the parts of the organization that will be impacted. The goal is to make sure that both your team and the vendor are on the same page when issues arise.

"How well do you understand my enterprise workload?"

The potential issues surrounding enterprise system migration and management can be complex, with many dependencies. A vendor with limited expertise and true understanding of your systems and strategic goals may only be able to address some of the challenges, leaving it to your team to ensure a safe, smooth transition.

Look for solid ISV relationships and enterprise computing experience

A long history with an ISV indicates that the cloud services provider understands older, legacy versions and deployments of that ISV's systems, as well as legacy hardware. Such a provider is better positioned to determine how to effectively deploy and manage those specific workloads in the cloud. Also scrutinize the relationship carefully: details matter. For example, a vendor that claims to be an SAP partner may have only achieved certification as a hosting provider, not as a full managed services provider.

Expertise

Understanding not just the cloud itself, but the workloads running on it

"Do you have a proven methodology?"

With each cloud migration, vendor knowledge increases. Not all vendors have the expert resources, or the processes, to tap into that insight or translate it into effective migration and management methodologies. This can create bottlenecks, with the vendor having to "learn as they go" to some extent, solving problems that may have already been addressed.

Look for a history in the enterprise space

Unlike newer vendors, well-established strategic enterprise partners are able to leverage lessons learned in previous deployments, both legacy and cloud-based. A vendor able to efficiently and safely help you transition to the cloud should have a proven methodology and "run book" that outlines potential issues and solutions specific to your workload. By understanding what's likely to happen ahead of time, avoidance and faster resolution when issues do arise become possible. The vendor should also use its own tools to gain insight about the workload, as well as those from third parties and ISVs to simplify migration.

"Do you have workload management expertise in diverse environments?"

Many managed cloud vendors are specialists, with expertise limited to their own infrastructure. When it comes to complex deployments that extend beyond their cloud offering, they must rely on third parties to help configure, shift and manage workloads. This adds complexity to vendor relationships, with no assurance of consistency across the managed environment.

Look for broad-ranging expertise

Different workloads associated with your enterprise systems, such as dev/test and production environments, are likely to be deployed using a variety of cloud infrastructures. Your needs may span management of enterprise workloads only (on an unmanaged cloud), management of both workload and cloud infrastructure, and cover public cloud, private cloud, legacy infrastructure, or any combination. To achieve consistency and reduce complexity, the cloud vendor should be able to deliver the same level of expertise and knowledge for any deployment contingency.

Global presence

Housing data and applications where regulations and business requirements dictate

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, secure cloud on a truly 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.

Global presence

Data and applications where regulations and business requirements dictate

Questions to ask about global delivery

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

Compliance and 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 impact critical SLAs.

Look for a global data center network

The provider should have data centers owned and operated by its own staff in all 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 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.

Global presence

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 secure 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 guarantee 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. You should know who is providing the infrastructure, ensuring its availability and safeguarding your data. Also look for assurances that your data will not be shifted from its specified location, unless you ask for it to be moved.

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
- 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

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:

A wide choice of compute, storage and network configurations that are highly flexible, scalable and available, from fully virtualized to bare metal, supporting Linux, Windows and IBM AIX and multiple database and middleware options

Migration consulting and assistance that speed the move of key workloads to the cloud

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

Disaster recovery on a global scale with failover and fallback

Compliance services that can help you 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 understands the beginning, transition and destination in your journey to the cloud

More and more, enterprises like yours turn to cloud managed services for help in transitioning to the cloud and to derive greater business value from enterprise applications and data. IBM Cloud Managed Services builds on our long experience in cloud, enterprise computing, security and business transformation to help make that journey smoother and quicker. IBM is a partner able to assist 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 enterprise applications like SAP in the cloud
- Continuous optimization of the cloud

Unlike IBM's comprehensive managed services, other providers' solutions have multiple moving parts. Some may use multiple, specialized partners to cover all the infrastructure and management services you need. Others may not be able to deliver the quality of enterprise application and data management that prompted your move to a managed cloud in the first place.

Businesses surveyed by Frost & Sullivan in 2017 gave IBM managed services a 97% approval rating.[5]

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

Choice

- ☐ What's your track record in mission-critical enterprise computing?
- ☐ Can you support my choice of technology and deployment model?
- ☐ Can you deliver everything I need – infrastructure, platform and managed services, consulting and AI capabilities?

Security

- ☐ Is your physical and IT security up to my standards?
- ☐ Where does your responsibility for security and service levels end – and mine begin?
- ☐ How good are your disaster recovery capabilities?

Management

- ☐ When you say you manage my environment – exactly what are you managing?
- ☐ Am I dealing with one company or several?
- ☐ How good – and how extensive – is your enterprise application support?
- ☐ Do you provide flexibility in management? Can I choose which tasks I manage and which I want you to take on?
- ☐ Do you provide a dedicated project executive who is my point of contact?
- ☐ What SLA's do you provide and are they guaranteed?

Expertise

- ☐ Can you demonstrate a proven and repeatable methodology for cloud migration and workload management?
- ☐ Do you have experience with my specific enterprise workload?
- ☐ Is your expertise in-house, or do you rely on third parties for some management tasks?
- ☐ Does your expertise extend beyond management of cloud infrastructure?

Global presence

- ☐ Can you meet my needs on a global scale?
- ☐ Can my data and workloads be placed where I need them?
- ☐ Do you require the assistance of third parties to achieve coverage where I need it?
- ☐ Are there extra charges for network costs when moving data across data centers?

Take the next step

Find out more about IBM Cloud Managed Services

Visit IBM Cloud Managed Services >
https://www.ibm.com/cloud-computing/infrastructure/managed-cloud-hosting

Request a consultation with an IBM Cloud professional >
Find out more about how managed services can help you. Visit http://ibm.biz/Cloud_SAP-Scheduler to request a no-charge, 30-minute consultation with an IBM expert.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
December 2017

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

[2] *Managed Cloud Services: Research to explore adoption patterns, challenges, benefits and expectations for managed cloud services: Final report.* Frost & Sullivan. July 6, 2017

[3] Ibid.

[4] *Are Cloud Managed Services Right For Your Business?: Creating a Successful Business Case.* Frost & Sullivan. 2017

[5] *Managed Cloud Services: Research to explore adoption patterns, challenges, benefits and expectations for managed cloud services: Final report.* Frost & Sullivan. July 6, 2017

GMO14218-USEN-04