



ESSENTIALS FOR BUILDING PARTNERSHIPS IN THE CLOUD

How to Identify a Qualified MSP,
CSP or Reseller

TABLE OF CONTENTS

Introduction	3
Managed Services Partner Selection Process	3
Review MSP Processes and Certification	4
Depth and Breadth of Offerings	4
Tools and Partnership	5
Roadmap	6
Incorporating Security	6
Team Size and Team Certifications	7
Conclusion	8

INTRODUCTION

With the evolution of various cloud computing models like Infrastructure as a Service (IaaS) and Platform as a Service (PaaS), organizations are becoming accustomed to the operational expenditure model (OpEx) and are leaving behind the capital expenditure model (CapEx) that was so heavily relied upon in the past. OpEx started with the public cloud providers' pay-as-you-go model, but it is now moving into managed services operations. Organizations are trying to avoid investing in operations teams for various reasons, ranging from hiring, training, tools licensing, etc., because having an operations team maintain an organization's cloud infrastructure creates management overhead.

Managed service providers (MSPs), cloud solution providers (CSPs), and other resellers make life easier for organizations by eliminating the need to maintain operations teams. MSPs provide continuous support for the ever-evolving cloud architectures, allowing organizations to focus on their core business goals rather than on managing operations. MSPs also serve as trustworthy advisors to organizations, helping them manage their day-to-day IT requirements.

Most MSPs have cloud offerings models that organizations can leverage for security, operations, and cost benefits. These offerings accelerate the technology adoption rate and provide complete transparency to customers. MSPs possess technical expertise and tools across various cloud platforms, and they are able to provide quick turnaround guidance for continuous architectural improvements. The next generation of MSPs is going beyond delivering services; now, they also foster relationships with customers and treat the customers' infrastructure as their own.

This white paper reviews some of the key points that organizations should consider when they are choosing an MSP.

MSP SELECTION PROCESS

MSPs can offer many benefits, but only if the right company is chosen for the job. MSPs come from a wide range of backgrounds. Some of them come from enterprises that have been in business for decades, while others are just entering the market and have the most up-to-date knowledge. As one might expect, there are advantages and disadvantages for MSPs on both ends of the spectrum.

There are many factors that organizations need to take into consideration in the process of finding the right MSP. We discuss some of the most important elements organizations should look for below.

REVIEW MSP PROCESSES AND CERTIFICATION

If there is one essential requirement for managing services operations smoothly, it is well-defined and implemented processes and procedures. Processes and procedures help MSPs maximize efficiency and service-level agreements (SLAs), which are necessities for any organization. Policies should cover incident, change, problem, vulnerability, and security incident management so that there will be clearly defined processes for handling each of these components. For efficient service delivery, MSPs should focus on knowledge base, runbooks, configuration information, asset/inventory information, etc.

Various industry standards such as [Information Technology Infrastructure Library \(ITIL\)](#), [PRINCE2](#) (Projects In Controlled Environments), and [ISO/IEC 27001](#) provide guidance for industry best practices in managing IT operations. The adoption of one industry standard puts organizations on the path to instituting other standards since there will be natural overlap between them. By implementing these standards, MSPs improve operations management and delivery. They aim to provide improved efficiency, greater power, cost reduction, and process standards.

When organizations are choosing an MSP, they should carefully review the processes that the MSP implements. There are some certifications bodies that can actually provide such certifications after carefully examining all of the executed processes. MSPs use these standard certifications as a selling point. Also, there are companies that publish their own [best practices checks](#), which an MSP can leverage to strengthen its offerings.

View the latest MSP Partner Validation Checklist.

[Read More ▶](#)



In addition to these certifications, cloud providers such as AWS and Azure should be able to present their auditing certifications and [public cloud provider competencies](#). For example, AWS released a [validation checklist](#) for the [AWS Managed Services Program](#), which has been used to evaluate AWS partners. If an AWS partner qualifies based on this checklist, AWS releases the AWS Managed Services Partner certification to the partner. These audits happen every year, which ensures that AWS partners maintain high standards. Gartner has also released their [Managed Services Providers Quadrant](#), which serves as a simple guide for organizations to identify the top MSP vendors in public cloud infrastructure space.

DEPTH AND BREADTH OF OFFERINGS

One of the standard practices organizations should follow before choosing an MSP is validating whether that MSP meets their requirements. Validation starts with identifying the right cloud provider for infrastructure needs, which then leads to a decision about which MSP fits those infrastructure needs. There are many MSP options around the world, so organizations should carefully examine the breadth and depth of services provided by the available MSPs.

The majority of MSPs focus on specific verticals (with the exception of enterprise MSPs), and their core offerings evolve around those verticals. For example, some MSPs are primarily focused on financial customers, while others specialize in HIPAA customers in life sciences and health care verticals. Even though there is a shared services vector across all of the verticals, vertical uniqueness is what differentiates one MSP from the others. Organizations should look for an MSP that has the correct specialization and the right set of product offerings/services to meet their particular needs.

In most cases, MSPs offer various support models, such as standard or enterprise models, which provide options for organizations to pick and choose from to ensure that the services align with their requirements. Organizations can also give their custom requirements to an MSP and see how the MSP responds to these demands. The new generation of MSPs can use opportunities like this to their advantage because customers pay for feature offerings while they are still being developed. Once corresponding offerings have been developed and standardized, MSPs can bring them to their existing customers and solidify their presence.

In addition, organizations should validate that the [service level agreement \(SLA\)](#) provided by an MSP aligns with their business requirements. A minute of downtime can result in millions of dollars lost, so they should examine the SLAs carefully and document the penalties associated with failing to meet them.

TOOLS AND PARTNERSHIP

To emphasize the previous point about determining the depth and breadth of MSPs' services, organizations can evaluate further by reviewing the tools MSPs use to support their operations. The tools can provide a quick capability overview for a specific area of services.

Let's take infrastructure monitoring as an example. There are various open-source and proprietary solutions available on the web and in the marketplace. Open-source tools provide open standards and are cost-effective, but they come with minimal support and increased business risk. On the other hand, proprietary software is expensive, but it offers more stability and support. Organizations should evaluate MSPs' tools to see if they meet ever-changing architecture requirements. For example, organizations should check to see if a given tool will provide the same functionality after migration from standard VMs to containers.

Just as organizations need to choose MSPs with the right tools to speed up their operations, MSPs must select the proper tools to support their business and provide solutions for their customers. In most cases, next-generation MSPs leverage other third-party SaaS or hosted applications to strengthen their offerings rather than developing in-house products. These offerings range from monitoring solutions, to unified threat-management tools, to deep inspection solutions. This wide range of offerings comes at an additional cost, but it helps MSPs meet their customers' dynamic requirements.

An MSP's relationship with specific vendors and cloud providers is an indication of the level of depth the MSP can offer. Most vendors and cloud providers have many, defined levels. For example, AWS has three levels for their ISV partners: standard, advanced, and premier. An MSP's partner status demonstrates their ability to provide adequate solutions. Organizations can validate the reputation of an MSP by reviewing their third-party partnership levels and confirming the credibility of their offerings.

ROADMAP

Technology and organizational architectures are continuously changing. As important as it is for organizations to align their architectures and applications with their growing customer requirements, it is equally essential for MSPs to continuously expand and enhance their offerings to keep up with evolving architectures.

For example, just a few years ago, VM-based architectures were very common, but now the focus has shifted to microservices architectures. MSPs need to change their offerings to meet new requirements and also ensure that internal and external processes continuously evolve. During evaluation periods, organizations should watch and see how their prospective MSP partners develop their offerings. They should check the services roadmap for their MSPs and validate that they are actually changing with the times. It is certainly important that an MSP's services meet an organization's current requirements, but it is equally necessary for the MSP to demonstrate that they are committed to providing continual improvements and keeping up with changing technology.

MSPs help organizations achieve smooth operation, but they also serve as advisors. Organizations must evaluate whether MSPs' architects are entirely knowledgeable about the changing technology landscape, and whether they can provide timely guidance on design best practices. MSPs that can meet these expectations will help organizations optimize their environments for cost, operations, and security.

INCORPORATING SECURITY

Security is the critical area of concern for any organization. They should carefully examine MSPs' security procedures and processes before handing over the keys to their infrastructure. Another essential validation criteria is transparency. Organizations should ensure that they have complete visibility into the environment while they share the keys with an MSP.

Organizations can also identify a qualified MSP by examining their access management procedure. Customers need to be sure that their chosen MSP will be able to prevent unauthorized access to their environment. Organizations should ask these questions to be sure that the right security controls are in place:

- › How will MSP team members access customer environments?
- › How will MSPs secure the devices used by their team members?
- › Which security audit controls are in place?
- › From which locations will MSP team members access the environment?
- › How will MSPs ensure that customer information is not shared with another customer?
- › Will MSP team members sit in a restricted area, and is a clean desk policy in place?

In addition to these security questions, organizations should validate MSPs' business continuity processes. Organizations should not put all of their eggs in one basket. Like cloud architecture, operations should be designed for failure. An environmental eruption in a single region should not break down the entire organization's operations. Accordingly, MSPs should have a BCP policy ready to go in case any issues arise.

Last but not least, organizations should review how MSPs handle breaches. Breaches can occur for various reasons, such as a buggy application code, open permissions, an S3 bucket that was accidentally left open, etc. MSPs will be the first to know about issues, so their initial response to these problems is critical. Organizations should determine whether there is a defined, transparent process for handling breaches, and that all team members in the MSP are appropriately trained.

TEAM SIZE AND TEAM CERTIFICATIONS

Another vital point to consider in the selection process is the MSP's team. Organizations should review how MSPs teams are spread across various roles, and should ensure that teams have clear roles and responsibilities defined for every position. This not only helps MSP team members, but it also helps customers establish expectations for each layer. Since most MSPs operate in a shared resource model, team training and maintaining a strong knowledge base is critical. Other significant aspects that organizations should consider are as follows:

- › Does the MSP have the proper resources to support their operations?
- › Does the MSP have backup resources in place?
- › How does shift handover work?
- › What are the various shift timings?
- › Does the MSP provide a technical point of contact for the project?
- › Does the MSP have a project manager for the project?

Finally, organizations should review MSP team members' certifications. This is essential because specialized knowledge may be needed across the environment, and MSPs should have experts who are able to understand the context from end to end.

CONCLUSION

Organizations should conduct the MSP selection process very carefully. Multiple team members should participate in the process so that each of them can assess the MSP's fitness to meet their specific needs.

MSPs have a powerful impact on an organization's success. They can help achieve constant growth. Organizations should be upfront about their expectations, and they should look for an MSP that is honest about its offerings and potential developments for the future. Even though the MSP might not have specific capabilities at the moment, they can use this information about what their customers need as an opportunity to further enhance their future offerings.

CloudCheckr's Channel Partner Program enables MSPs, Cloud Solution Providers (CSPs), and other resellers to sharpen their competitive edge in this competitive market.

An MSP that partners with CloudCheckr can incorporate industry-leading Best Practice Checks into its product offerings, simplify business operations, increase profit margins, and become more attractive to prospective clients as a qualified reseller. [Learn more about the Channel Partner Program here.](#)

Need CloudCheckr for your organization? Learn more at www.cloudcheckr.com.



342 N GOODMAN ST,
ROCHESTER, NY 14607

1-833-CLDCHCK

www.cloudcheckr.com