



A guide to moving your application or solution to the cloud.

igroup

© 2019 INTELLIGENCE GROUP LTD (T/A IGROUP)

Microsoft
Partner



Gold Cloud Platform
Silver Cloud Productivity
Silver Small and Midmarket Cloud Solutions
Silver Application Development
Gold ISV



© 2019 Intelligence Group Ltd (T/A igroup)
A guide to moving your application or solution to the cloud.

All rights reserved. No part of this publication text may be uploaded or posted online without the prior written permission of the publisher.

Authors: Garry Forsyth and Sarah Scott

Contents

Introduction	3
Chapter 1 - The plan	5
First steps are daunting	5
Goals	5
Platform	5
Chapter 2 - The detail	7
Networking	7
Disaster recovery	8
Software Updates	8
Security	8
Authentication & Authorisation	9
Antivirus/Malware	9
Monitoring	9
Configuration	10
Chapter 3 - The migration	11
Service	12
Costing guide	13
Chapter 4 - Takeaways	15
MoSCoW	15
There's No One-Size-Fits-All Approach	15
Get Advice from the right people	15
Appendix A – Regions	18
Appendix B – Platform Limits	19
Resource Group Limits	19
Storage Accounts	19
Virtual Networks	20
Virtual Machines	20
Appendix C - Terminology & reference notes	21

Introduction

The cloud is an amazing but complex platform and making the most of it can be difficult without experience.

Achieving desired resilience, performance, availability, access, security, scalability and disaster recovery capabilities without incurring hidden costs or barriers further down the line should be your businesses ultimate focus.

The business risk to moving your software product or service to the cloud is significant. There's so many variables to consider. So much could potentially go wrong, and at the end of the day, your software is part of, or possibly your primary business function. You can't afford any hiccups or failures and that's why so many businesses haven't either made that leap, or worse, have abandoned their cloud project.

In this guide, we address general technical concerns and how to tackle the knowledge gap, explain cloud components, how they fit together, comparing traditional infrastructure to cloud infrastructure, and which cloud services are best suited to software providers.

Challenges software providers face today

Most software providers have common goals at the most basic business level - to evolve your solution and stay ahead of your competition, grow your customer base, and increase revenue and profit. And to do that, your solution must be delivered over a stable platform.

Each of these areas presents a challenge to overcome which can be tackled by varying main stream solutions. But very few of those solutions can address all those challenges. The cloud can.

Is the cloud affecting business growth?

Many of today's software giants such as Microsoft and Adobe, have successfully deployed their product via the cloud many years ago. Their software solutions are now that established, stable, and feature rich in the cloud environment, an expectation has been set with the consumer to access all software online.

Despite this major change within the industry, small to medium software vendors are still situated within their own onsite infrastructure, co-location, or managed hosting, and can still be unaware of the gains that can be had by choosing to move their solution to the cloud.

Benefits can include regular income from monthly user subscriptions, closer control of licenses, and the ability to manage and deploy software versions directly to the end user.

By choosing to deliver your software solution via the cloud, it offers easier access to the end user, enabling faster purchase decisions and instant and repeatable revenue for your business.

But you also gain more insight into your end users and the ability to report on activity, enabling you to assess areas of your solution that might need improvement, identify successful features that could be developed more or monetised, such as leveraging extra fees for heavy usage of your software or new features and tools.

Gains from infrastructure improvements

The largest gains, we believe, are from the platform itself which primarily relate to business savings, but also touch on increasing growth.

The challenges faced managing platforms and infrastructure are sporadic and consequently, issues such as security and outages are not generally invested in or measured in the same way.

Consider, for example, a server failure in a colocation centre. It's something that you have a contingency plan for, but would it have an accurate cost to the business allocated? Think about the man hours involved to drive there and back to your colocation centre with new equipment that you've invested in which is sat on standby, and the time it takes to perform a physical swap out.

Regulatory compliance is another area of your software solution that takes considerable time to manage, implementing and maintaining different policies. The more compliance you have in place, the larger your addressable market becomes.

At the point when business success requires your infrastructure to grow, you're faced with further investment in servers because you can only scale horizontally, requiring further rack space, storage, redundancy, cooling, and power to name but a few.

There's also the time it takes to solve performance issues, general management of the servers and their platform, ensuring security and the disaster recovery plan is up to date.

The cloud addresses all of these problems to varying degrees, providing significant benefits that are not immediately realised. Yet it's still not widely embraced, provoking the ultimate question, why is that?

What's stopping your project getting off the ground?

There's many reasons why cloud projects don't get off the ground but when you analyse the objections raised, you find several key culprits that reoccur each time.

A lot of businesses prefer to do things in-house, even when it comes to managing IT infrastructure. Typically, software providers will utilise existing resource such as developers to maintain traditional infrastructure because of the familiarity with the technology. However, cloud technology is such a vast subject, the knowledge people have around it can be limited, even for developers.

To overcome this challenge, either new skills need to be learnt, which distracts your key employees from performing their role to look after your product or you need to consider hiring in skills.

You are then faced with how to choose the right cloud service for your software solution, working out your monthly billing might be based on your architecture and usage as well as the complex licensing, building your new architecture to at least meet if not exceed your current performance levels, how you'll migrate to it, and finally maintain your new infrastructure and platform. You also must consider the continued challenges of resolving unknown issues between your software and the infrastructure.

What's stopping you from getting your software into the cloud?

Chapter 1 – Building your plan

First steps are daunting

The number of variables you must plan for in any physical infrastructure change is vast but compared with the move to something that's a brand-new concept to a business, and possibly yourself too, those variables multiple exponentially.

Preparation and research is key to a smooth transition to the cloud. But we're not just talking about reading up on Amazon AWS or Microsoft Azure's websites.

Goals

You may only be thinking about moving one aspect of your business to the cloud, but we've found that most businesses are pleasantly surprised by the results and choose to migrate more of their business almost immediately after.

Taking the time to scope your full business requirements and create a phased plan now, means that you will have the right architecture in place, available to scale when you're ready. It's always an eye-opening exercise for any company too!

But you also need to think about your company's primary goals. What is it you are trying to achieve through this process?

- Replace on-site hardware which you must maintain with more flexible, usage-based cloud resources which can be maintained by the provider?
- Do you have plans for growth or business structure changes?
- Is your current colocation provider delivering poor performance? Are service and/or outages causing you headaches?
- Does security need to improve?
- Or costs be reduced?

Having goals keeps your project focused.

It's all obvious preparation but it's surprising how often one or more of these areas are overlooked, impacting on project deadlines and spending valuable resource working out what's gone wrong.

Platform

Choosing the right platform is crucial. It can affect business costs, scalability, your application, and potentially your clients to name but a few.

If you find that you are struggling to identify the right platform or service in the cloud, or maybe not even thought about it – that's ok. Really. It is.

The services in any cloud are rarely 1:1 feature equivalent with their non-cloud counterparts meaning it's difficult to do a comparison. What most businesses don't realise, is that the

platform described as the perfect solution in the providers literature isn't cost effective or sometimes even workable and it certainly won't offer up the alternative ways to achieve the same outcome.

Realistically, unless you have a cloud expert in your team, and by that, we mean someone that's completed multiple deployments focused around software applications, you're going to struggle to pick the right one for your business.

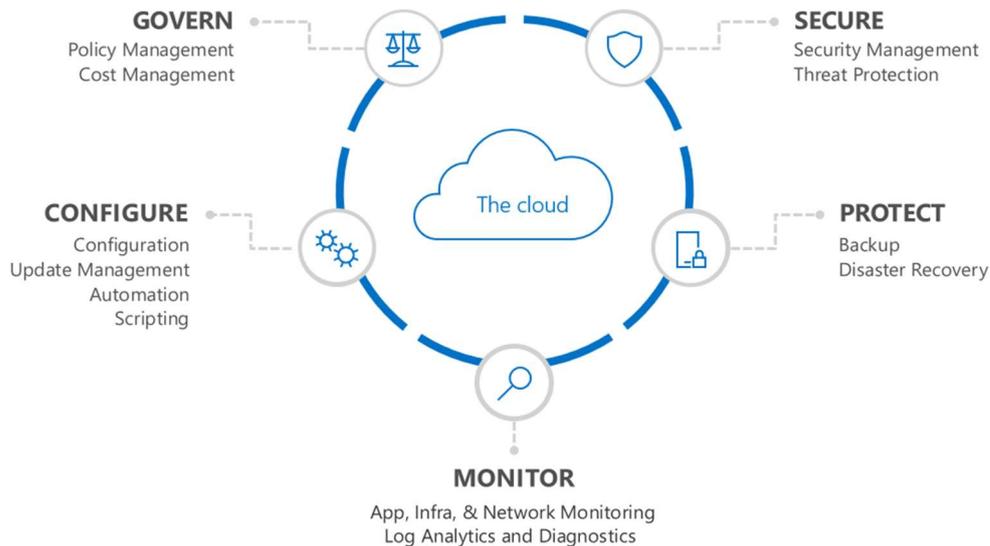
It's quite common to find that software vendors have homed in on PaaS before they approach us. PaaS is ideal for software written for a particular providers platform, not legacy code.

The service most established vendors end up using is IaaS because it's easier to transition existing code, it's cloud agnostic and doesn't require current existing proven and fully tested code to be re-written specifically for a single cloud provider, adding unnecessary risk, unless there is good reason.

For this reason, we've focused this white paper around that.

Chapter 2 – Infrastructure component detail

The cloud provides a lot of services and features which help to reduce the effort and skills required to deploy services and applications.



But even with these services in place, there is more to running and managing Infrastructure as a Service (IaaS) than assumed or fully disclosed by cloud providers as some services may not be included as default, at all or could even be an additional significant cost.

igroup have been running Infrastructure as a Service (IaaS) in the form of virtual machines on Microsoft Azure since 2011 and Amazon Web Services since 2016. During this time, we've discovered that many services required for traditional, on-premises, VPC or co-location services, also apply to our resources in the cloud.

We have grouped the services into eight main categories and highlighted myths, wrong assumption, and best practice:

- Networking
- Disaster Recovery
- Software Updates
- Security
- Authentication & Authorisation
- Antivirus/Malware
- Monitoring
- Configuration Management

Networking

The cloud provides some great networking functionality, but it's still important that any deployment of a Virtual Network is planned correctly, and networking experts are consulted in a similar way as would be for a new data centre's network.



Disaster recovery



There's a lot of resilience and reliability within the cloud; but these features are often assumed incorrectly to provide disaster recovery.

For instance, any data or infrastructure placed with a cloud provider is at risk of data corruption or even data loss and provisions should be made for this.

Our team always recommends that clients use as much of their existing disaster recovery procedures and investments as possible so that recovery procedures of cloud resources are as close as possible to your proven and familiar recovery plans to support consistency of management/operations.

If you require additional functionality, providers like Microsoft Azure do provide Recovery Services in the cloud for Virtual Machine snapshots which can be backed up to another region and recovered as Virtual Machines directly on Azure but there are additional costs to this service and the MTTR can be higher than on-premise solutions and existing business SLAs.

Software Updates

In both AWS and Azure, you can make use of the Operating System Images the cloud provider offers. You automatically receive the latest updates of the Operating System when you deploy the virtual machine.

However, after deployment, it's your responsibility to manage and monitor software updates for both the Operating System and any additional software you may have deployed.

Security



The cloud provides some level of defence when it comes to Security. We've used Microsoft Azure as detailed example of what's covered, but the same principles apply to AWS:

- **Encryption:** Azure uses industry standard protocols to encrypt data as it travels between devices, Microsoft data centres, and communication within data centres.
- **Secure Networks:** Azure Virtual Networks provide private networks in the Azure cloud.
- **Threat management:** Microsoft uses intrusion detection, denial-of-service (DDoS) attack prevention, penetration testing, data analytics and machine learning to constantly strengthen its defence and reduce risks.
- **Compliance:** The cloud complies with international and industry-specific compliance standards and participates in rigorous third-party audits. (For full details about Azure see: <https://www.microsoft.com/en-us/trustcenter/Compliance>) (For full details about AWS see: <https://aws.amazon.com/artifact/>)

What's not clear though, is security at the Operating System level and above for IaaS and service/endpoint level and above for PaaS is still your responsibility, including public internet security if any ports are opened on public IP addresses.

In terms of exposure, this still leaves the majority of security-related risks with your business.

Authentication & Authorisation

Authentication and authorisation is the most common service overlooked when people are thinking about deploying resources to the cloud.



For example, if we look at access to the management interfaces on Microsoft Azure, it's typically secured using Azure Active Directory Services, but access to the Virtual Machines or applications on the Virtual Machines themselves is often overlooked.

Although it is work in progress and supported in some edge cases, the most common misconception about Azure Active Directory is that it can be used for all Authentication and Authorisation services (AD Domain Servers) in Azure, but this isn't the case – you should consider your IaaS as simply another of your data centres so that all risks can be assessed, and requirements produced before choosing a product/service for your security services. Convenience is rarely the most practical or secure solution.

The same applies to AWS, although terminology varies for the product names, the features and principles are the same.

Antivirus/Malware

When you deploy Infrastructure as a Service (IaaS), you are responsible for everything from the Operating System upwards, which includes Antivirus/Malware.



As with many of the other services, we would always recommend using your existing investments in Antivirus/Malware if possible for consistency and familiarity reasons.

Alternatively, if you've chosen Azure, it does have an optional feature on VMs for Antivirus/Malware, but they will result in additional costs.

Monitoring

Although cloud providers offer a basic level of monitoring such as:

- CPU Utilisation
- Memory Utilisation
- Network Bandwidth
- Port Monitoring



Most businesses require something a bit more sophisticated and certainly something that will provide more historical data and allow the creation of reports and/or alerting.

If this is the case for your business, extra budget will be required, but it is possible. You'll require a server/infrastructure monitoring solution much as it would for on-premises or utilisation of additional Azure services such as OMS, Log Analytics and Diagnostic Data services or AWS services such as Amazon Inspector and Amazon Guard Duty.

Configuration



All the services we've talked about in this section, along with the provision of the services initially, typically require some level of configuration management to ensure everything is deployed correctly.

You can make use of the individual services each provider offers. For example, Azure has a very good PowerShell API for provisioning/updating services running on Azure and it is recommended that all deployment and updates are made through this API so that the scripts can be bundled into change scripts.

However, configuration of the Operating System, deployment of software and software changes all need to be handled externally. This is usually done using the same tools and software that that you may already be using on traditional server infrastructure such as: would be used on-premise:

- System Centre Configuration Manager (SCCM)
- PowerShell Desired State Configuration (DSC)
- Group Policy/Login Scripts
- Configuration Orchestration Software

Chapter 3 – Migrating, maintenance, and costs

There's lots of factors to also consider around a migration too as well as ongoing maintenance.

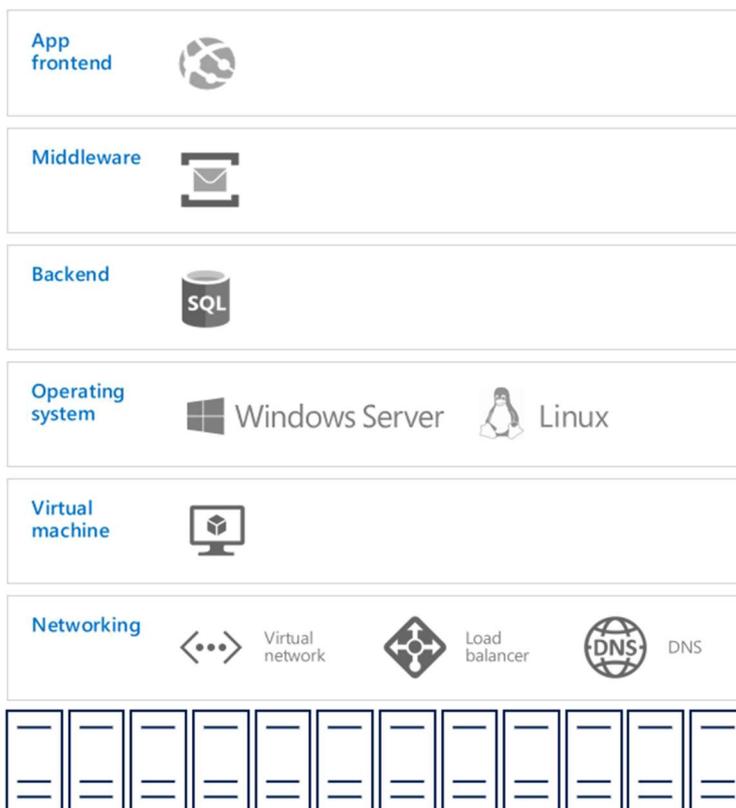
What's your situation? Where are you moving from and too?

- Own data centre to a cloud provider or via a cloud vendor
- Traditional / Colocation to cloud provider or via a cloud vendor
- A data centre that's already in the cloud to the cloud provider direct or via another vendor specialising in cloud
- One cloud provider to another (eg move from Azure to AWS)
- A cloud provider to a cloud vendor (eg move from AWS, to AWS or Azure through Rackspace or igroup)

Your situation will have the biggest impact to your migration plan.

Whatever your situation is, the same underlying principals still need to be considered when you're planning your migration.

- Consider what you are currently responsible for?
- What will you be responsible for on the new environment?
- How will you manage new additions?
- How will your customer be affected?
- Are there cost implications?



Service

The most common option businesses lean towards is moving directly to the cloud provider (Azure or AWS), but boundaries for responsibility aren't always clear. Depending on what platform (IaaS or PaaS) or service is selected, can affect what your business will be responsible for.

We've created a breakdown to help explain.

	Traditional			Cloud		
	Own Datacentre	Colocation (own servers)	Colocation (rented)	IaaS	PaaS	IaaS (igroup)
Applications	●	●	●	●	●	●
Data	●	●	●	●	●	●
Runtime	●	●	●	●	×	◇
Middleware	●	●	●	●	×	◇
Security Patching	●	●	●	●	×	◇
Anti-Virus/Malware	●	●	●	●	×	◇
OS	●	●	●	●	×	◇
Networking	●	●	◇	●	×	◇
Virtualization	●	●	◇	×	×	×
Servers	●	●	◇	×	×	×
Storage	●	●	◇	×	×	×
Network backbone	●	◇	◇	×	×	×
Rack Space	●	◇	◇	×	×	×
Power Distribution	●	◇	◇	×	×	×
Cooling	●	◇	◇	×	×	×
Physical Access & Security	●	◇	◇	×	×	×

Key

●	Your business	◇	Your cloud provider (Azure or AWS)	×	Your traditional infrastructure or cloud vendor (igroup or Rackspace)
---	---------------	---	------------------------------------	---	---

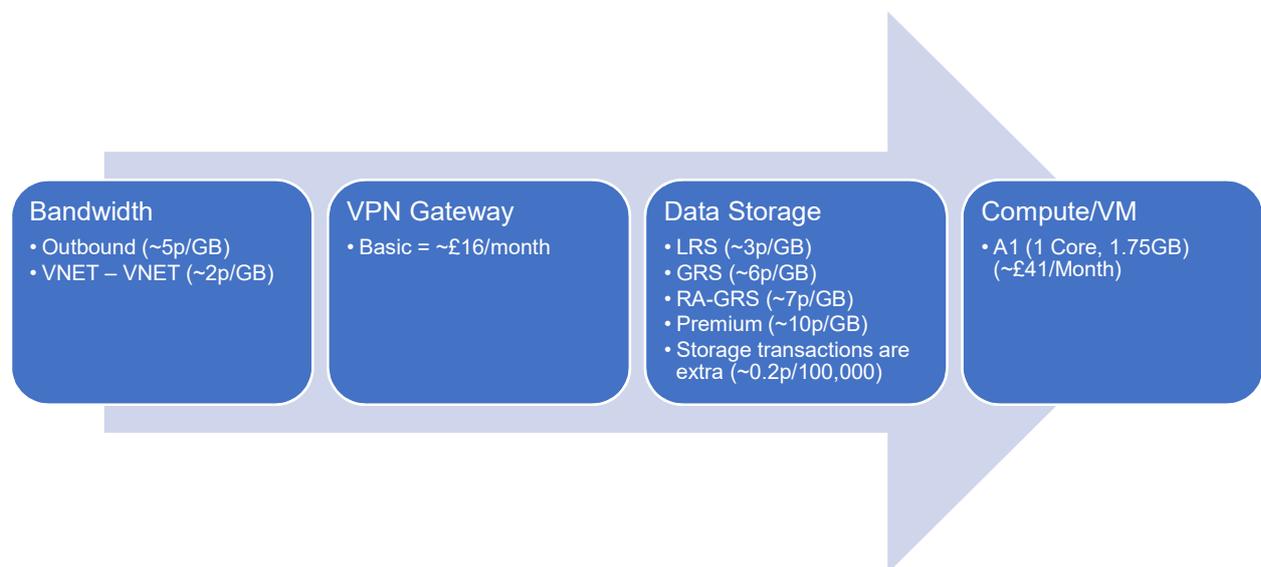
Costing guide

Costing for the cloud can become quite complicated very quickly due to the number of meters, resources and different prices for different resources in different regions.

The information below is based on Microsoft Azure and provided as a guide to the relative costs of the different resources and should be viewed as estimates for generic example purposes only.

Infrastructure as a Service (IaaS)

As a guide, the diagram below gives an idea of where the most significant costs typically are for an Azure subscription, where the cost increases from left to right.



Platform as a Service (PaaS)

Infrastructure as a Service (IaaS) involves the purchase of resources such as bandwidth, networking, storage and compute. The resources you purchase are allocated, which means the utilisation of them is controlled by you e.g. if you have a Virtual Machine you can use as much of the CPU and Memory as you need up until the maximum you purchased. Typically for IaaS, once you reach the limit you will notice performance issues.

However, Platform as a Service (PaaS) is different. Microsoft manages the IaaS resources on your behalf to provide a consistent service at a consistent performance level or SLA. Microsoft, therefore, throttles your access to the service purchased performance level to ensure you do not exceed this and to ensure your access to the service does not impact other customers. This is important because your service won't simply slow down, it will always perform at the same level or queue up requests if you exceed the agreed performance level(s).

Therefore, pricing for the PaaS services is typically provided at fixed service levels involving some arbitrary unit which Microsoft has designed to reflect the resources the services uses.

Typically, the more resources (CPU, Network, Storage) required by your service the higher the cost. Unfortunately, because the resources are attributed through an arbitrary unit, it is often not possible to predict the performance/service level or relate this to an on-premise equivalent because the details of the unit are not available and therefore testing should always be performed when using PaaS to ensure you are aware of the level required for your application as costs differences between service levels can have large impacts on budget requirements. Also, be aware that bandwidth/data transfer will still be charged for PaaS services and for some services storage will also be applicable unless it is included in the services plan.

Chapter 4 – Takeaways

MoSCoW

Establish your goals and needs. What **must** you have, **should** you have, **could** you have, and **would** like to have. From here, a good advisor will be able de-risk your project and deliver an affordable and flexible solution that achieves your requirements.

There's No One-Size-Fits-All Approach

When it comes to evaluating any potential cloud service, researching and identifying a possible concept is easy—there's plenty of material to sell you the dream.

Here's two key facts that are not shared with the marketing materials found online by providers and vendors. First, those services are generally targeted in the first instance at businesses with none legacy code, and second, taking that theory and putting it into practice is a completely different matter and is not supported by the cloud provider.

There isn't a 'how to' guide to download or free online technical support from Microsoft or Amazon to help you through a 'step by step'. You are on your own, surrounded by a wealth online documents that may help or hinder you.

Get Advice from the right people

Choosing a vendor that has your businesses best interests at heart is a challenge, just like buying any other product or service. Here's some of our best tips on how to select one.

The cloud is a service, but it's not that easy to change further down the line like swapping energy providers, so it's important to get it right as early as you can. Finding a provider that highlights help on the path to the cloud rather than the end goal of hosting is more likely to offer honest advice about what's best for your business.

Look for a provider that offers a menu of services that you can select from. If they're offering that flexibility of choosing how much help you require and most importantly, not insisting to host through them, you can be confident the result will reflect your business goals.

Providers who are cloud agnostic, offering more than one of the cloud solutions available today, again, increase your chances of a well-balanced engagement.

Remember, your chosen provider should be placing your application / solution first, working with you to understand how your software works before suggesting services or platforms. You shouldn't have to adapt your software for the cloud. Adapt the cloud services and architecture to your application.

The bigger the provider, the less advice you get. It's sad, but true. After all, it's not in the interest of a big provider to offer advice for clients of every size during onboarding.

You should be offered alternative options of how to achieve your goal. There's so many parameters to choose during configuration – that's why most businesses need advice. So, if you're only being offered one solution, question why, and if you have doubts, get a second opinion. Any company worth their weight, should be able to offer that.

Our best advice is to have a look at what's out there, but then seek advice before committing.

How igroup can help you

We've worked with many software providers, assisting in the reinvention of their business into the cloud and because of that experience, we've been able to create a unique set of services perfectly suited to that market sector.

The services are available as a menu, giving you the freedom to choose how much help we provide. Each service is also flexible, so you can create a truly personalised consultative experience which is affordable and supported by actual experts.

Our services will help de-risk your project, provide a personalised approach, ensuring your chosen solution is right for you, and provide the right level of support that your business requires.

De-risking the project

Why eat into your business margins? We find so many software providers considering carrying out the move internally. Your developers should develop, not migrate, create and maintain servers.

The temptation to use your technical team to work on this challenge probably won't have factored in that it is a large learning curve, and there's plenty of room to potentially get several aspects wrong.

Those wrong decisions won't stop your move and they may not even hinder it at first. But there's a strong probability they'll cause infrastructure and cost problems further down the line. It's one of the things we've learnt from many clients—getting it right first time saves money.

Having access to that technical experience to optimise environment, budget, performance, architecture, and availability, as well as best practice to manage monitoring, security, network management, patching is invaluable. Picking the right service and vendor will help you balance those costs for all attributes to deliver the best possible solution for you.

Flexible approach to suit your goals, not ours

We help engineer a balanced solution that can work for you, with services created with flexibility in mind. Your cloud migration plan and proposed architecture should complement your businesses goals and timelines.

During a consultation process, we advise what services you'll benefit from most, but we will also look to tailor each of those services to ensure you get the result you require.

Choosing the right options for your budget

We're flexible, independent, and agnostic - we'll tell you if there are cheaper options. How many companies have you already spoken to that have tried to lock you in to a hosting contract through them? Or encourage you to use a cloud manufacturer?

To us, choosing a cloud provider is like choosing a commodity or brand. At the end of the day, it's your choice and all we can offer is our best advice. Choosing a vendor to supply that commodity is again, another choice. And again, all we will do is offer our best advice and all the options available through us or direct with the providers.

Actual support not lip service

Support in your time zone from 3rd line experts that will help you solve slow server problems and work out if a problem sits with infrastructure or software.

igroup started out as a software developer. Today, we support a lot of software vendors in their journey to the cloud and their tenancy, but we've also been a software vendor developing apps in our early days and since 2010, hosting and maintaining customised SharePoint installations for businesses across the UK.

Our support isn't read from cue cards via first line support like many mainstream providers. It's delivered by 3rd line experts specialising in infrastructure as well as development. They've been with us since our early years and take immense pride and pleasure in helping our clients. We recognise that this is an important part of our service because it's regularly commented upon from almost every new customer.

Appendix A – Regions

Continent	Azure Region	Location
Americas	East US	Virginia
	East US 2	Virginia
	Central US	Iowa
	North Central US	Illinois
	South Central US	Texas
	West Central US	Wyoming
	West US	California
	West US 2	Washington
	Canada East	Quebec City
	Canada Central	Toronto
	Brazil South	Sao Paulo State
	Europe	North Europe
West Europe		Netherlands
France Central		Paris
France South		Marseille
UK West		Cardiff
UK South		London
Germany Central		Frankfurt
Germany Northeast		Magdeburg
Southeast Asia		Singapore
East Asia		Hong Kong
Australia East		New South Wales
Australia Southeast		Victoria
Australia Central		Canberra
Australia Central 2		Canberra
China East		Shanghai
China North		Beijing
China East 2		Shanghai
China North 2		Beijing
Central India		Pune
West India		Mumbai
South India		Chennai
Japan East		Tokyo, Saitama
Japan West		Osaka
Korea Central		Seoul
Korea South		Busan

Appendix B – Platform Limits

Below are a selection of the platform limits for general services and IaaS services, for a complete list by service type please see <https://docs.microsoft.com/azure/azure-subscription-service-limits>.

Resource Group Limits

Resource	Maximum Limit
Resources per resource group (per resource type)	800
Deployments per resource group	800
Resources per deployment	800
Management Locks (per unique scope)	20
Number of Tags (per resource or resource group)	15
Tag key length	512
Tag value length	256

Storage Accounts

Resource	Maximum Limit
Number of storage accounts per subscription	200
TB per storage account	500 TB
Max number of blob containers, blobs, file shares, tables, queues, entities, or messages per storage account	Only limit is the 500 TB storage account capacity
Max size of a single blob container, table, or queue	500 TB
Max number of blocks in a block blob or append blob	50,000
Max size of a block in a block blob or append blob	4 MB
Max size of a block blob or append blob	50,000 X 4 MB (approx. 195 GB)
Max size of a page blob	1 TB
Max size of a table entity	1 MB
Max number of properties in a table entity	252
Max size of a message in a queue	64 KB
Max size of a file share	5 TB
Max size of a file in a file share	1 TB
Max number of files in a file share	Only limit is the 5 TB total capacity of the file share
Max 8 KB IOPS per share	1000
Max number of files in a file share	Only limit is the 5 TB total capacity of the file share
Max number of blob containers, blobs, file shares, tables, queues, entities, or messages per storage account	Only limit is the 500 TB storage account capacity
Max number of stored access policies per container, file share, table, or queue	5
Total Request Rate (assuming 1KB object size) per storage account	Up to 20,000 IOPS, entities per second, or messages per second
Target throughput for single blob	Up to 60 MB per second, or up to 500 requests per second
Target throughput for single queue (1 KB messages)	Up to 2000 messages per second

Target throughput for single table partition (1 KB entities)	Up to 2000 entities per second
Target throughput for single file share	Up to 60 MB per second
Max ingress per storage account (US Regions)	10 Gbps if GRS/ZRS enabled, 20 Gbps for LRS
Max egress per storage account (US Regions)	20 Gbps if RA-GRS/GRS/ZRS enabled, 30 Gbps for LRS
Max ingress per storage account (European and Asian Regions)	5 Gbps if GRS/ZRS enabled, 10 Gbps for LRS
Max egress per storage account (European and Asian Regions)	10 Gbps if RA-GRS/GRS/ZRS enabled, 15 Gbps for LRS

Virtual Networks

Resource	Default limit	Maximum Limit
Virtual networks per subscription	50	500
DNS Servers per virtual network	9	25
Private IP Addresses per virtual network	4096	4096
Concurrent TCP connections for a virtual machine or role instance	500K	500K
Network Interfaces (NIC)	300	10000
Network Security Groups (NSG)	100	400
NSG rules per NSG	200	500
User defined route tables	100	400
User defined routes per route table	100	400
Public IP addresses (dynamic)	60	contact support
Public IP addresses (Static)	20	contact support
Load balancers (internal and internet facing)	100	contact support
Load balancer rules per load balancer	150	150
Public front end IP per load balancer	5	contact support
Private front end IP per load balancer	1	contact support
Application gateways	50	50

Virtual Machines

Resource	Maximum Limit
Virtual machines per availability set	100
Certificates per subscription	Unlimited

Appendix C - Terminology & reference notes

Before you get started, take a quick glance at our mini glossary to help clarify who or what we're talking about.

Provider – Microsoft Azure, Amazon Web Services (AWS), Google Cloud Platform.

Vendor – a business that provides a service through one or more provider (group are a vendor).

Business, Client, Customer – meaning you, the customer.

Platform – Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS).

Service – Azure SQL, Cloud Storage, Managed Database Services, Compute, Networking, Web Apps.

Acronym	Category	Description
SaaS	Software as a Service	SaaS is software which is hosted for end users to access via the cloud or as an API for a bespoke application. There is no management or upgrading involved.
PaaS	Platform as a Service	PaaS takes away the requirement to manage the underlying infrastructure such as software maintenance, patching, capacity planning, and resources. You only focus on deployment and management of your application or solution.
IaaS	Infrastructure as a Service	IaaS provides access to the basic building blocks required for IT infrastructure such as networking, computers (such as Virtual Machines or Networks), and data storage. It offers the highest level of flexibility and management and is a structure that is most relatable to traditional IT infrastructure. You are responsible for the management of the IaaS environment unless you look to outsource to a cloud vendor.



Gold Cloud Platform
Silver Cloud Productivity
Silver Small and Midmarket Cloud Solutions
Silver Application Development
Gold ISV

