Korcomptenz

Microsoft

Understanding cloud migration strategies

Barry Briggs

Published by

Contents

1. Introduction: The promise of the cloud

There's no denying it: in the past few years cloud computing has become mainstream, with over 90% of organisations deploying workloads to the public cloud, according to a number of studies (for example, RightScale's State of the Cloud).[1]

And why not? The cloud promises many benefits not only to IT departments, but to the organisation as a whole. Initially seen as a way for companies to cut computing costs, today the cloud is unlocking whole new benefits, including resiliency, security,

scalability and especially *agility* both for IT and for the business. Companies once hoping simply to reduce costs are finding their businesses transformed as they rely more and more on the cloud.
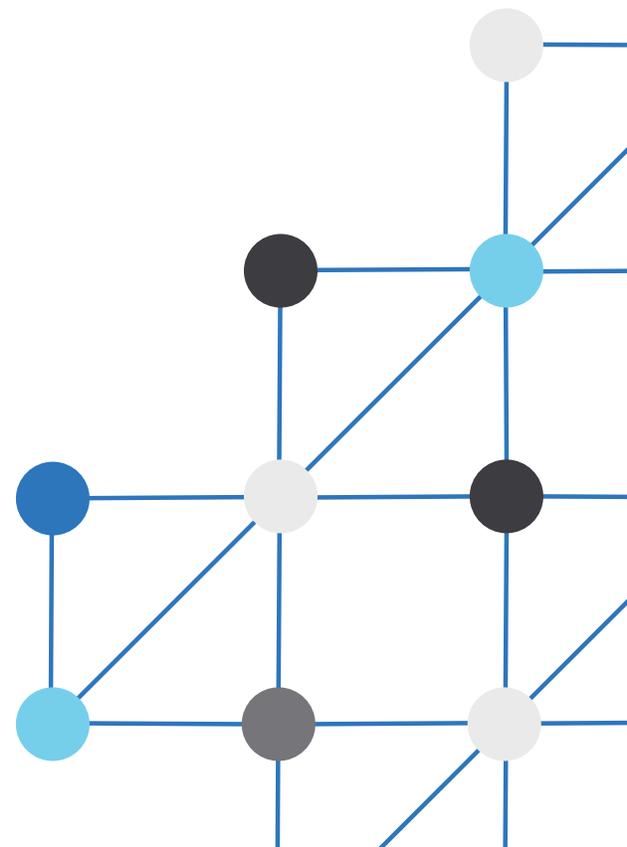
[1] 'RightScale 2019 State of the Cloud Report from Flexera.' Flexera, February 27, 2019. https://www.flexera.com/about-us/press-center / rightscale-2019-state-of-the-cloud-report-from-flexera-identifies- cloud -adoption-trends.html.

Increase business agility with the cloud

For years, Allscripts,[2] a leading healthcare software manufacturer, wanted to build a solution to help doctors locate the lowest-cost drug prescription source for patients – but at nearly a million dollars, the development hardware alone made the business case untenable.

But in the cloud, the development resources cost just 34 USD per day! Moreover, the team had access to a number of high-value cloud services such as databases, integration services, and others – with just a few clicks – speeding the delivery of the solution.

Companies everywhere are discovering that with the on-demand, pay-as-you-go nature of the cloud they can quickly and inexpensively create new capabilities and respond rapidly to emerging business opportunities.

Cut costs with cloud computing

Datacentres are expensive, with the costs of real estate, power, servers, storage, and networks, plus operations staff tugging on a company's bottom line, so it's no wonder that organisations see the cloud as a way to reduce or even eliminate some or all of these expenses. For example, Dutch insurance company Zilveren Kruis Achmea[3] cut hosting costs by *50%*!

How? They took advantage of the cloud's ability to automatically scale up to handle high-traffic periods – and scale down when demand decreases. No longer are they weighed down by expensive servers sitting idle.

[2] 'The Allscripts Prescription for Agility: Lift and Shift to the Cloud.' Microsoft Customer Stories, May 7, 2018. https://customers.microsoft.com/story/allscripts-partner-professional-services-azure.

[3] 'Cloud Migration Helps Zilveren Kruis Cut Infrastructure Costs by More than 50% for Mission-Critical Application.' Microsoft Customer Stories, June 24, 2019. https://customers.microsoft.com/story/725384-zilveren-kruis-insurance-azure-devops-netherlands.

Improve security with the cloud

Companies like Accenture,[4] the Hearst Corporation,[5] and HCL Technologies Ltd.[6] rely on the advanced security technologies found in the public cloud to protect themselves against an ever-changing threat landscape.

Today, Microsoft spends over 1 billion USD annually on security, with more than 3,500 security professionals and a host of cloud-based security technologies and products – the fruits of which are available to all its customers.

Use the cloud to create new business models

Rolls-Royce[7] collects and analyses telemetry data from its more than 13,000 commercial aircraft engines currently in service – using cloud-based Internet of Things (IoT) and artificial intelligence services. As a result, they are able to proactively identify potential problems requiring maintenance long before they become issues – and can now provide their engines 'as a service', where customers are charged by the flying hour, rather than as a capital expense.

With the ability to collect and analyse massive amounts of data in real time, the cloud is one of the principal drivers of many such changes in how business is done: something that is called 'digital transformation'.

[4] 'Accenture Safeguards Its Move to the Cloud with Microsoft Cloud App Security.' Microsoft Customer Stories, August 29, 2018. https://customers .microsoft.com/story/accenture-professional-services-cloud-app-security.

[5] 'Eight Things This Media Giant Likes about Microsoft Enterprise Mobility + Security and Azure Active Directory.' Microsoft Customer Stories, June 3, 2019. https://customers.microsoft.com/story/726295-hearst-media-and -cable-enterprise-mobility-and-security.

[6] 'HCL Technologies Uses Enterprise Mobility + Security to Delivery Highly Secure Digital Workplace.' Microsoft Customer Stories, April 2, 2019. https://customers.microsoft.com/story/hcl-partner- professional -services-microsoft-365.

[7] 'Rolls-Royce and Microsoft Collaborate to Create New Digital Capabilities.' Microsoft Customer Stories, August 10, 2019. https://customers.microsoft.com/story/rollsroycestory.

What's the 'hyperscale' cloud all about?

At its core, the cloud consists of massive amounts of compute, storage and networking power distributed across the globe, all available for customers to use, as much or as little as they need, whenever and wherever they need it – which is what we mean by 'hyperscale'.

Today, Microsoft Azure is available in 54 regions worldwide for 140 countries,[8] as shown in the illustration below. More are being added as this is being written.

---

[8] 'RightScale 2019 State of the Cloud Report from Flexera Identifies Cloud Adoption Trends.' Flexera, February 27, 2019. https://www.flexera .com/about-us/press-center/rightscale-2019-state-of-the-cloud-report -from-flexera-identifies-cloud-adoption-trends.html.

Figure 1-1. Microsoft Azure regions

Migrating to the cloud

No doubt then that the many promises of cloud computing are compelling. But many organisations hesitate with their first step: moving their applications from their datacentres to the cloud. That is the subject of this book.

To begin with, let's take a look at some key cloud computing concepts and terms that will serve as the basis for formulating and executing a migration to the cloud. First, we'll quickly cover the various types of cloud: private, hybrid and public; then we'll discuss the different ways of running applications in the cloud, from 'lift and shift' to 'cloud-native' approaches.
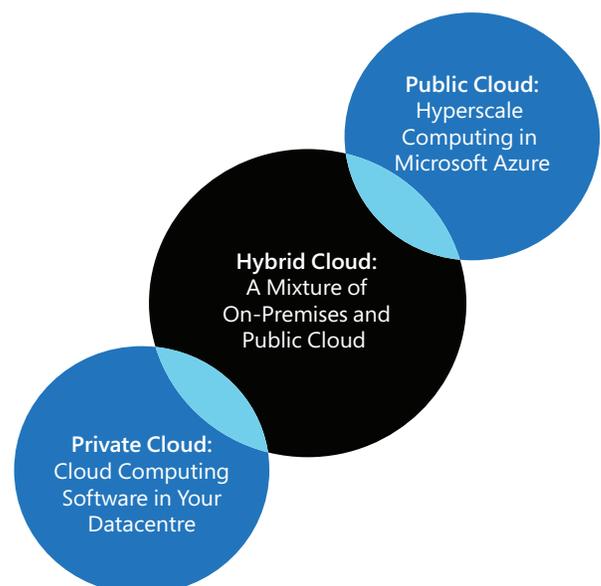
Public Cloud: Hyperscale Computing in Microsoft Azure

Hybrid Cloud: A Mixture of On-Premises and Public Cloud

Private Cloud: Cloud Computing Software in Your Datacentre

Figure 1-2. Private, hybrid and public clouds

Private cloud

In a *private cloud*, cloud technologies are hosted in an on-premises datacentre, with large numbers of commodity hardware running identical system software: in other words, a 'cloud' that belongs to you. Private clouds can be useful because they can implement a technology stack that is consistent with the public cloud. This might be necessary in scenarios for which certain applications or data cannot be moved off-premises, or when network connectivity is unreliable or non-existent.

For the general case, however, companies find private clouds to be of limited utility. They do not provide the cost savings and efficiencies that the public cloud can, because private clouds require a significant capital expense budget and an operations staff; thus, they remain on your balance sheet. Moreover, individual companies cannot achieve the economies of scale of a public cloud provider that we described above, so their costs are proportionately higher.

Finally, private clouds do not possess the 'hyperscale' nature – capacity-on-demand – that the public cloud boasts. Still, as we suggest, there are very specific scenarios in which a private cloud is useful, or even essential.

Interested in how Azure can support VMware private clouds? Go to:

[Azure VMware Solutions guide](#). →

Public cloud

A public cloud, which is the focus of this book, is built, managed and maintained by a large technology vendor, which makes computing, storage and software available on a rental basis.

The leading public cloud vendors, including Microsoft Azure, have datacentres all over the world with millions of servers available for use. Customers (enterprises) can either take advantage of applications that already exist in the cloud or can upload their own proprietary applications, and, as we shall see, there are a number of ways in which applications can physically exist in the cloud, but appear private to the enterprise corporate network.

Hybrid cloud

Often, an enterprise will wish to keep some of its applications on-premises while moving others into the public cloud; and, of course, it is desirable that all these applications continue to run as they did before, that is, as if they were all still local and on the same network. When some applications are in the cloud and some are on-premises, it's a 'hybrid cloud'. Almost every enterprise will have a hybrid cloud at some point; even if they plan to completely move all their applications off-premises, there will be a time during which the transition occurs when some applications have moved and others have not: a hybrid model.

To securely connect the two environments, several solutions exist. A virtual private network (VPN) can be set up that will enable cloud applications to appear to be on the same internal network as the enterprise. VPNs can be set up on a per application basis or, with a hardware device, for the entire corporate ecosystem.

Alternatively, enterprises can purchase through their telecom provider a dedicated line (such as Azure ExpressRoute)[9] linking the corporate datacentre with the cloud; bandwidth can be purchased as needed. This solution is preferable when it is desired to keep all traffic off the public internet and/or when substantially higher bandwidth is required. However, it entails additional cost.
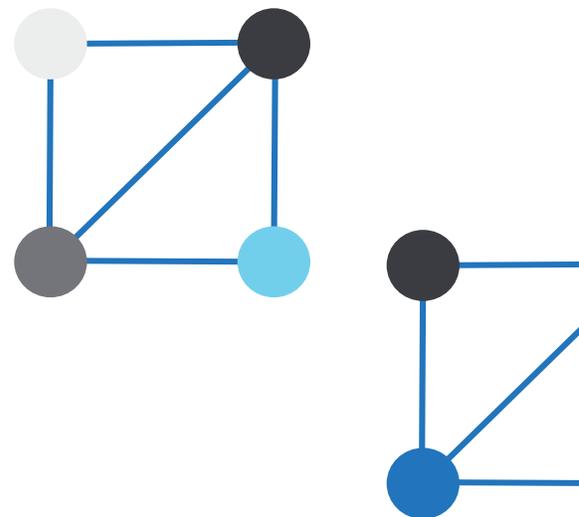
[9] 'Azure ExpressRoute.' Microsoft Azure. Accessed November 5, 2019. https://azure.microsoft.com/services/expressroute.

'As a Service'

As you consider migrating to the cloud, it's worth planning *how* your applications will be deployed.

As we'll show in the next few sections, the cloud offers a number of *application models* ranging from IaaS, which mirrors closely how applications run in the datacentre, to more advanced *cloud-native* architectures, which take advantage of the cloud's unique features.
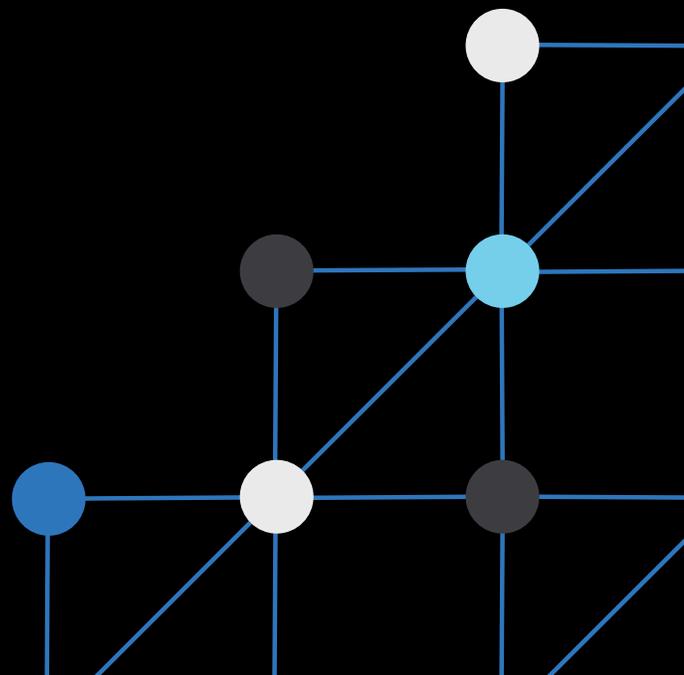
Infrastructure as a Service (IaaS)

In IaaS you are only renting the server hardware and a small amount of software (the hypervisor) to host your application's virtual machine (VM), where the VM consists of the operating system, associated system software and the application itself. With IaaS, VMs (or bare-metal servers) are simply *moved* from on-premises to the cloud in a process called 'lift and shift'. As shown in the illustration many operating systems and applications coexist on a cloud server; a thin piece of code called a 'hypervisor' ensures each VM runs in a timely and efficient fashion.

In other words, you supply – and maintain – the pieces in blue.

For much more detail about Microsoft Azure infrastructure offerings, go to the book

[Enterprise Cloud Strategy](): [Infrastructure]().
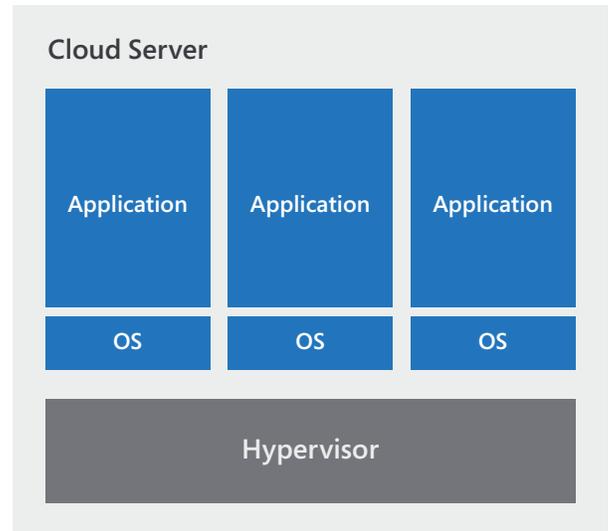
Figure 1-3. Infrastructure as a Service

This is the easiest and fastest migration strategy; the result is sometimes called a 'virtual datacentre' since it effectively replicates your applications in the cloud. Properly managed and optimised (we'll have more to say about that later), IaaS can result in significant cost savings. But, it still means that your operations staff will need to perform tasks such as patch management, updates and upgrades.

Nevertheless, IaaS is one of the most common cloud deployment patterns.

Platform as a Service (PaaS)

In PaaS, the cloud provider maintains all system software, removing the burden of upgrades and patches from the IT department. In a PaaS deployment model, the enterprise only needs to focus on deploying its code on the PaaS machines; the cloud provider ensures that operating systems, database software, integration software and other features are maintained, kept up to date and achieve a high service level agreement.
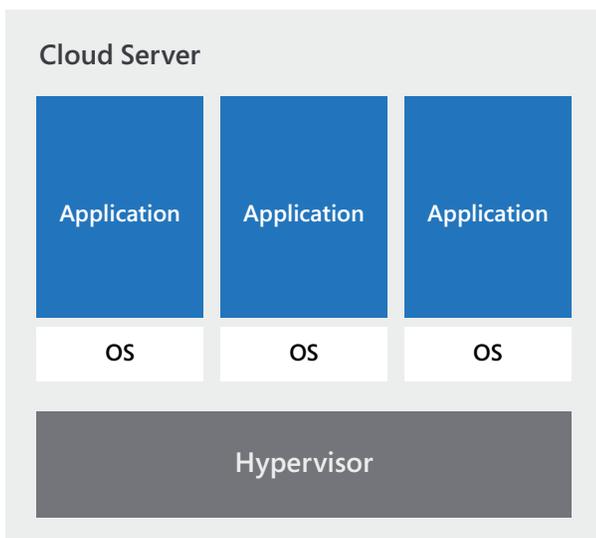

Figure 1-4. Platform as a Service

Note in this illustration the pieces in blue – the parts that the user must supply and maintain – consist *only* of the application.

PaaS provides IT departments with important benefits, most importantly the cost savings associated with reduced or eliminated maintenance of system software, and other rote functions. However, PaaS usually implies some redesign of the application in order to best take advantage of the model.

Software as a Service (SaaS)

In SaaS, you simply rent an application from a vendor, such as Microsoft Office 365 for email and productivity. This is by far the most cost-effective of all the options because the only work involved for the IT department is provisioning users and data and, perhaps, integrating the application with your company's single sign-on (SSO).

Typically, SaaS applications are used for functions that are not considered business-differentiating, for which custom or customised applications exist to operationalise competitively differentiating business models and rules.

When choosing how to move functionality to the cloud, be on the lookout for opportunities to use SaaS-based applications. Typically, they will provide you with the highest return on investment.
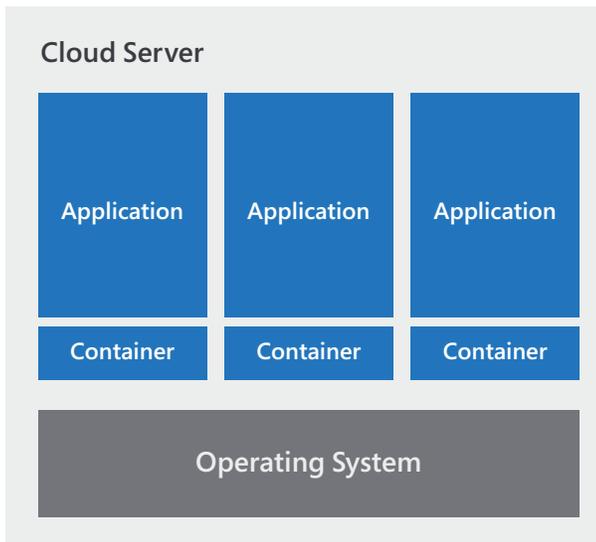
Figure 1-5. Container architecture

Containers

Containers – which lie somewhere between IaaS and PaaS on the 'as a service' spectrum – are a means by which applications can share a single instance of an operating system, which provides the appropriate isolation and security guarantees preventing applications from 'stepping' on one another. Because starting a containerised application typically does not involve loading and initialising an entire VM with an operating system, container start-up can be very fast – so scale up and scale down can be performant.

Containers have many advantages. Often it is possible to package an application with few or little changes to run inside a container, and it's useful to deploy multiple copies for scale or resiliency reasons.

A related technology, *orchestration*, can help automate the process of deploying many copies of many different applications or components to a *cluster* of servers.

Cloud-native computing brings all the benefits of the cloud

It's often the case that companies see the cloud as a 'virtual datacentre', that is, as an alternative and cheaper way to host their VMs. Over time, however, they recognise that the cloud offers unique capabilities, such as managed application orchestration, microservices, 'serverless' computing, a rich selection of managed database services, Internet of Things (IoT) services and machine learning (to name a few), which are available with just a few clicks.

With cloud-native computing, companies, instead of force-fitting the old VM model of computing into the cloud, can take advantage of built-in cloud features to achieve new levels of agility, scale, resilience and business capability. In this way, cloud computing is less of a destination – and more of a journey.

Migrating to the cloud: An overview

In this eBook we'll focus on how to migrate to the cloud. Companies that approach cloud migration strategically, that is, methodically, are the most successful in achieving their goals. Some of the steps which we'll cover later focus on how to develop a plan, prepare technical and organisational change management and carefully migrate with a strong strategy for governance.
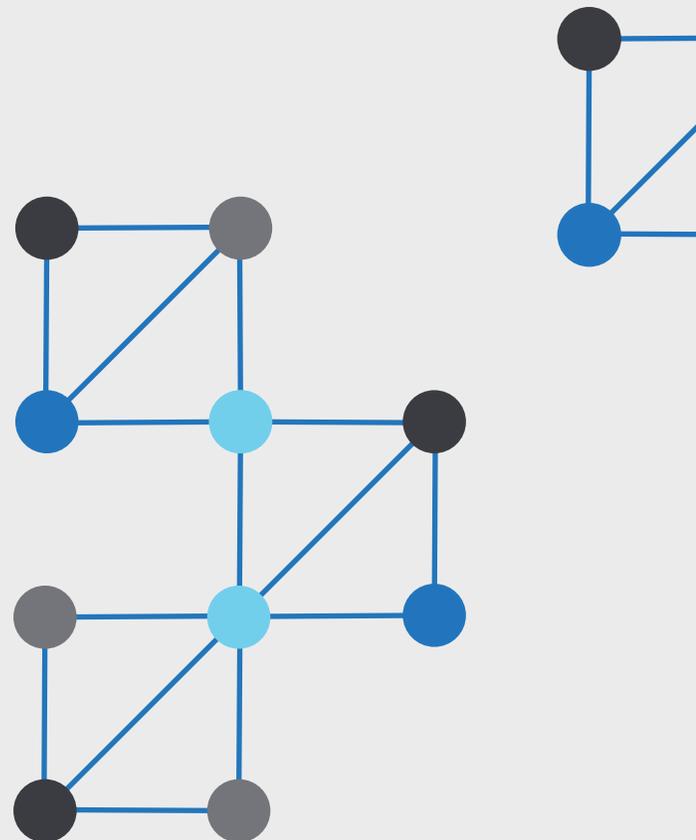
2. Planning your cloud migration

A successful cloud strategy takes into account the impact and implications of cloud computing across the entire organisation. In this chapter, we'll show the various dimensions of a cloud strategy and the steps you can take to ensure their success.

Understanding your motivations and defining the goals you expect to achieve in the cloud should be among the first steps you take in your cloud journey. Goals, of course, will help guide you – and your teams – as you progress.

As you define your objectives, quantify your definition of 'success' – for example, *decrease run costs by x percent by Q1*, or *close two datacentres within 12 months*. It's a good idea to add a time frame for goals to be achieved.
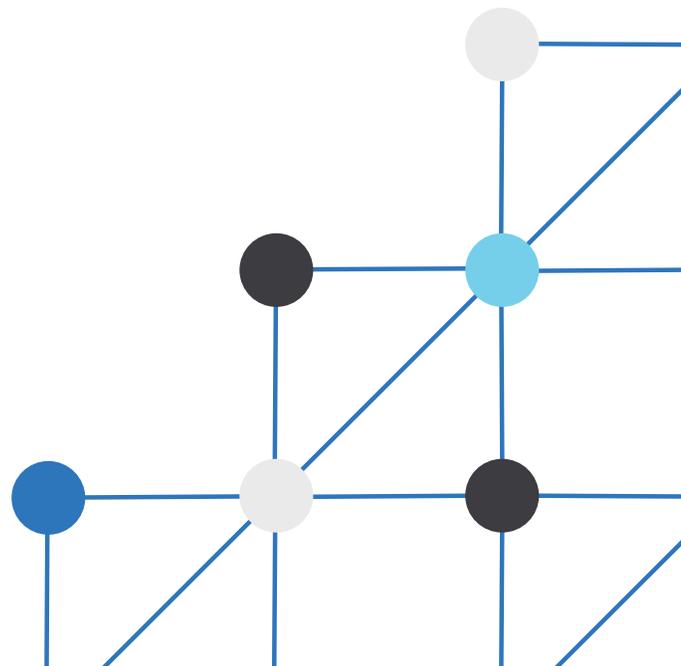
Setting your goals

What are your goals in the cloud? Many are possible; some include:

- **Business agility.** Reaching new markets; getting products to market faster; getting better, and faster, insights into customer needs and behaviours; and implementing new business models: all these are examples of how the cloud can help an organisation become nimbler and more responsive.

- **Reducing capital expenditures.** You pay for cloud services on a subscription basis so that the large capital expenses associated with on-premises computing – servers, networking equipment, software licences, and so on – and depreciation can be reduced or eliminated.

- **Consolidate and/or close datacentres.** Datacentres are expensive, entailing facilities, operations, environmental (air conditioning, humidity control) and physical security costs. Many companies maintain redundant datacentres for business continuity and disaster recovery purposes, at high cost. The cloud presents many opportunities for reducing a company's datacentre footprint.

- **Reducing risk from legacy applications.** When moving data to the cloud, it's a great time to think about application and systems software modernisation. For example, Windows Server 2008 reaches end of support in January 2020; moving these workloads to Windows Server on Azure is an optimal modernisation path.

- **Take advantage of cloud scale.** Microsoft Azure is a hyperscale cloud, meaning that resources are available as you need them. Want to collect data from thousands or even millions of IoT devices? Need to scale up during holiday periods and back down at other times? The cloud provides you the most cost-effective way to do this.

Odds are your goals will be some combination of those listed above. Consider involving your business partners in these discussions. Once aware of the possibilities, they might add business-focused goals, such as 'reach new markets in Asia within one year', or the like.

Like every major endeavour, you should also consider building a formal business case. Understand your expectations for how costs will evolve – your total cost of ownership (TCO), what your return on investment (ROI) is likely to be, and what costs you may encounter during migration.
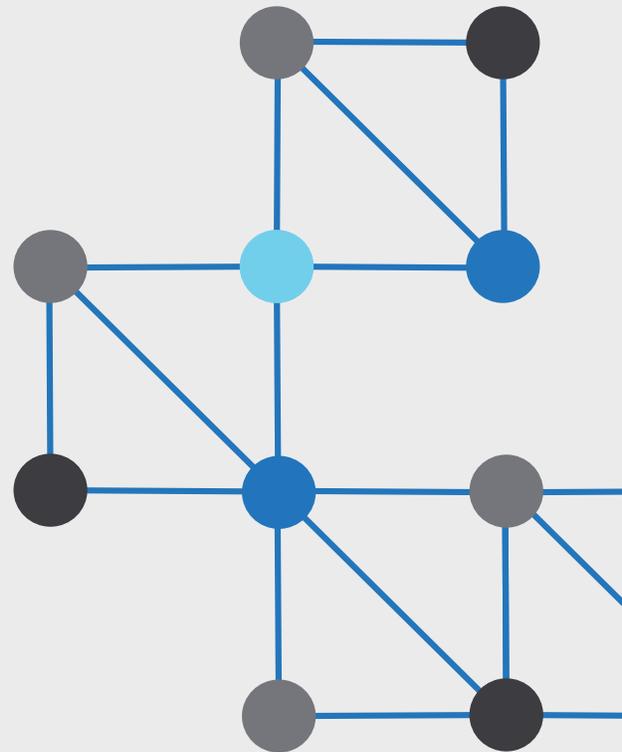
Want to know more about how to build a business case for the cloud? Go to the article:

Build a business justification for cloud migration. →

Build your cloud strategy team

The next step is to gather the individuals in your organisation who will lead your data migration to the cloud: *your cloud strategy team*. The primary charter for this team is to *build the roadmap*, that is, the plan for migration: to set priorities, manage expectations, ensure a smooth operation of the migration across all teams and measure progress against the goals. The team should include representatives from all major IT organisations as they will, in some way, be affected by the move to the cloud.

In addition to the roadmap, the cloud strategy team also builds (or facilitates building) the architectures, patterns and guidance for deployment of the re-envisioned applications or services. Finally, it manages the communications to key stakeholders and promotes the success and learnings from the program.

As shown in the diagram, include leaders – both managers and technical – from across the organisation, not only the delivery teams but also finance, security and risk management, and others. We'll have more to say about their specific roles shortly.

IT Management

IT Cx0

IT Security

IT Finance

IT HR

Cloud Strategy Team

IT Business Units

| Sales IT | Marketing IT | Manufacturing IT | Finance IT |
| HR IT | Support IT | Shared Services IT | Legal IT |

Figure 2-1. The cloud strategy team

Assessing your estate

As you begin moving your production applications, start by using (or creating) a catalogue of them, with attributes to describe their characteristics and peculiarities. This catalogue will form the basis of *prioritisation*, which we'll talk about in the next chapter.

Today, there are many tools available to help you automatically discover your applications and their readiness for moving to Azure; Microsoft provides an entire suite of functionality under the umbrella of Azure Migrate.[10] Azure Migrate is a hub for all your migration needs for Azure, and here you can choose between first-party Microsoft tools or third-party assessment tools.

If you have a portfolio management system to catalogue your applications, you should use that information as well. Tools such as Azure Migrate are specifically targeted at determining an application's readiness to move to Azure, where a portfolio management system may have other useful information, such as whether the application manages sensitive information.

In addition, a configuration management database contains useful information regarding the hardware and software components required by applications.

Go to the article to learn more:

[Azure Migrate](https://azure.microsoft.com/services/azure-migrate).

---

[10] 'Azure Migrate'. Microsoft Azure. Accessed November 6, 2019. https://azure.microsoft.com/services/azure-migrate.

Your application strategy

As you catalogue your applications, consider how you will deploy them to the cloud. IaaS, PaaS containers and SaaS offerings: all these, as discussed in the first chapter, have advantages and disadvantages.

Many companies adopt a strategy whereby most applications migrate in IaaS mode, at least at first, since it is relatively straightforward and requires little or no change to the application itself. Often, they also posit that all new applications and/or applications undergoing significant revision should be retargeted to cloud-native architectures.

Data classification

Many companies classify their data according to its sensitivity: a marketing document has a very different security requirement than, say, a draft of a 10-K filing prior to earnings release. Many organisations adopt a strategy by which the least sensitive data is migrated first.

Your data classification strategy should also take note of regulatory implications. For example, privacy laws such as the EU's General Data Protection Regulation (GDPR) limit where data about individuals can be stored. Your cloud provider can help here (see for example, the Microsoft Trust Centre).[11]

Creating a data strategy

As important as your application strategy (some would say more important) is your strategy for migrating data to the cloud. A cloud data strategy is composed of multiple dimensions, which we'll discuss in the next few paragraphs.

---

[11] 'Microsoft Trust Centre'. Microsoft. Accessed November 6, 2019. https://www.microsoft.com/trust-center.

Encryption

Consider creating policies by which your data is encrypted in the cloud. For example, you might (and probably should) adopt a policy by which sensitive data is encrypted while 'at rest' (on disk) and 'in motion' (i.e. using an encrypted protocol like HTTP/S).

Data management options

The cloud has a wealth of data management tools ranging from commercial relational databases such as Oracle and Azure SQL Database,[12] open-source RDMSs such as MySQL and MariaDB, as well as numerous so-called NoSQL databases such as Azure Cosmos DB,[13] MongoDB and others.

As you plan the migration of your relational databases, it's worth understanding the trade-offs of moving them into an IaaS VM or, alternatively, into a managed database service. If, for example, your database application uses legacy features or more complex capabilities like cross-database joins, it may be simpler to

migrate to IaaS first. Or to take advantage of cloud elasticity and scale, and to reduce management requirements, use a cloud-managed database.

For applications such as telemetry monitoring, clickstream analysis and security information and event management not requiring the overhead of a relational database, you may find a globally scalable NoSQL database to be both economical and useful. Such databases lend themselves well to managing huge capacities of data distributed across cloud regions and can be the basis of machine learning and artificial intelligence applications.

For specifics and case studies on how to migrate your database to Microsoft Azure, go to:

[Database Migration Guide](#). →

---

[12] "Azure SQL Database." Microsoft Azure. Accessed November 6, 2019. https://azure.microsoft.com/services/sql-database.
[13] 'Welcome to Azure Cosmos DB'. Microsoft Azure. October 22, 2019. https://docs.microsoft.com/azure/cosmos-db/introduction.

Cloud security

Keeping your applications and data safe from intrusion and breaches remains, of course, one of IT's highest-priority functions. As we mentioned earlier, your information security team should familiarise itself with the protections offered by the cloud provider, including

- **physical security** of the cloud datacentre, including background checks and biometric two-factor authentication for employees;

- **breadth of security offerings,** ranging from cloud anti-virus to distributed denial-of-service protection to encryption to key management;

- **identity and access controls** including secure directory and single sign-on; and

- **defence-in-depth** capabilities providing protection at every level of the stack.

Microsoft invests over 1 billion USD per year in security, with more than 3,500 security professionals. For more on how Azure is leading edge cloud security, go to the article:

Strengthen your security posture with Azure.

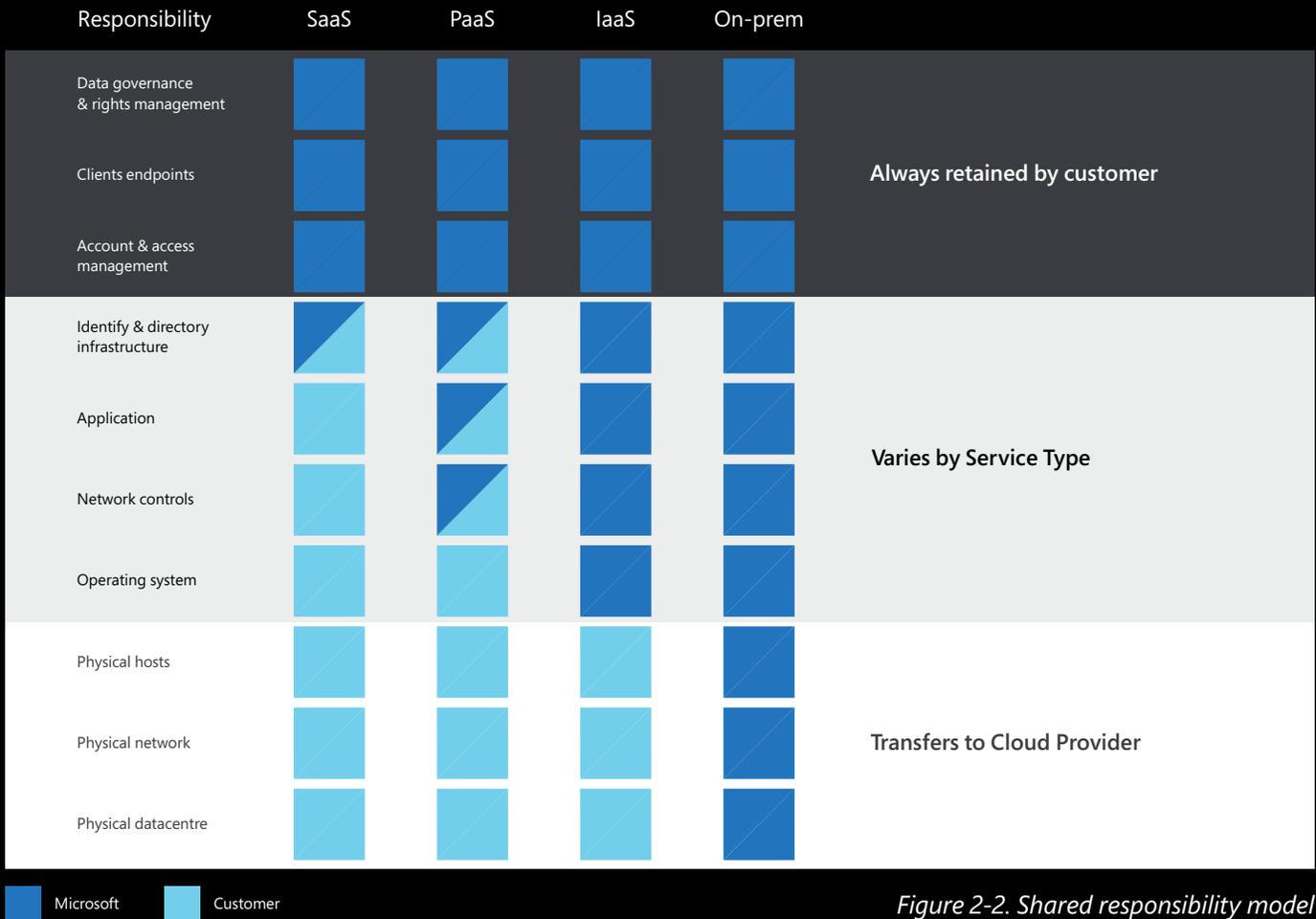| Responsibility	SaaS	PaaS	IaaS	On-prem	
Data governance & rights management					**Always retained by customer**
Clients endpoints					
Account & access management					
Identify & directory infrastructure					**Varies by Service Type**
Application					
Network controls					
Operating system					
Physical hosts					**Transfers to Cloud Provider**
Physical network					
Physical datacentre					

Microsoft   Customer

Figure 2-2. Shared responsibility model

As you plan your migration, it's important to understand the shared responsibility model[14] of both security and regulatory compliance in the cloud. By this term we mean that the cloud vendor, in our case, Azure, assumes some of the responsibilities of information security, while you are responsible for others.

For example, Azure and Microsoft are responsible for ensuring the security of their datacentres and, for managed services, system software. However, you as the customer retain responsibility for systems software (if you're using IaaS VMs) and for the security of your applications and data.

[14] 'Azure Infrastructure Security.' Microsoft Docs, October 17, 2019. https://docs.microsoft.com/azure/security/fundamentals / infrastructure#shared-responsibility-model.

Regulatory compliance

Compliance with national and local laws, as well as with industry standards, is also top of mind for IT executives, and with good reason, as non-compliance can result in severe penalties (GDPR violations can incur up to 4% of a company's revenues).

As with information security, cloud providers have adopted a shared responsibility model for compliance. Your cloud strategy teams should

- familiarise themselves with how the shared responsibility model applies to your specific industry (for example, US healthcare companies can use Azure and comply with the Health Insurance Portability and Accountability Act, or HIPAA);[15]

- also familiarise themselves with the cloud provider's overall posture regarding compliance, including understanding its list of certifications, its ability to work with governments and industries to shape regulations, and how it can help you develop your strategy.

Microsoft Compliance Manager provides a dashboard summarising your data protection and compliance recommendations.

Go to the article for more details. →

15 "HIPAA and the HITECH Act." Microsoft 365 Compliance offerings/Health. Accessed November 6, 2019. https://www .microsoft.com/trustcenter/Compliance/hipaa.
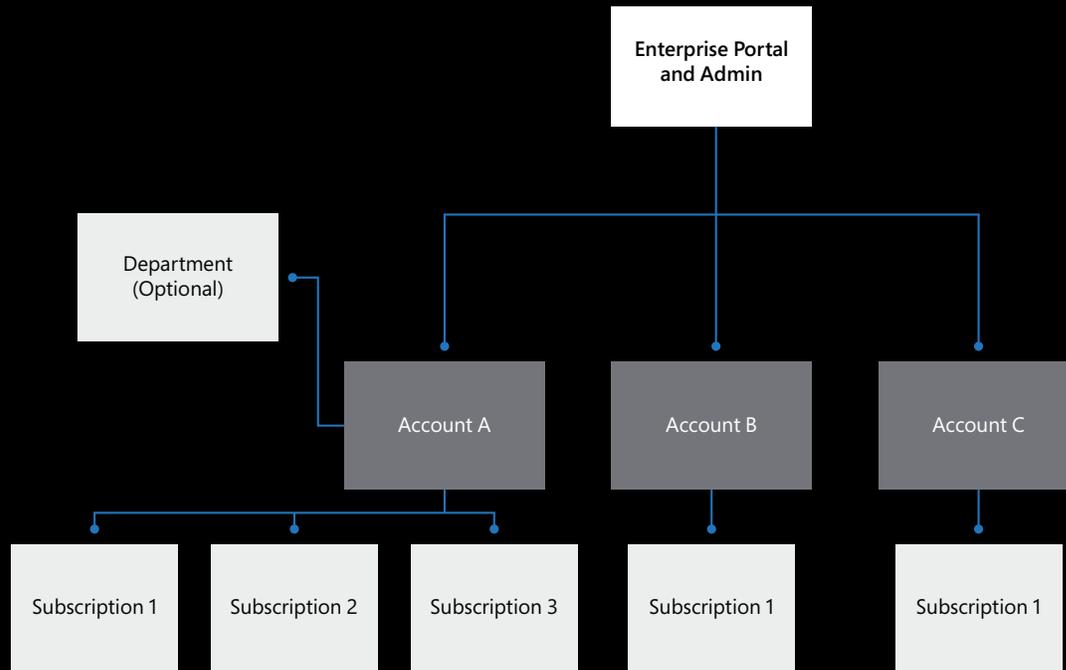
Figure 2-3. Subscription alignment

Developing a financial plan

Your finance team should be involved in planning from the beginning, as the overall paradigm for finance shifts – some would say dramatically – from a capital expense (servers, storage and network) to an operational expense, or 'rental' model.

In particular, finance professionals should:

- Help the organisation develop a subscription management model and tagging strategy. Companies typically find that having subscriptions at an organisational level (e.g. one for each IT business unit) simplifies management. Tags, applied to each resource deployed in the cloud, can also help associate each such resource with (say) a cost centre, thus improving accountability.

- Establish with these tools (subscription management and tagging) a chargeback process by which the organisations and teams using cloud services are charged appropriately for them.

- Help teams 'right-size' their deployments in the cloud, scaling down (and reducing costs) in periods of low traffic and scaling up in high-traffic times, for example, during holiday seasons for retailers.

- Understand how to get the best deals from the cloud provider, such as by taking advantage of Azure Hybrid Benefit[16] (to transfer on-premises software licences to the cloud) or reserved instances[17] (prepaid VMs), which can save up to 80% of cloud costs.

- Evaluate and use cloud cost management software available from Microsoft as well as from Microsoft partners.
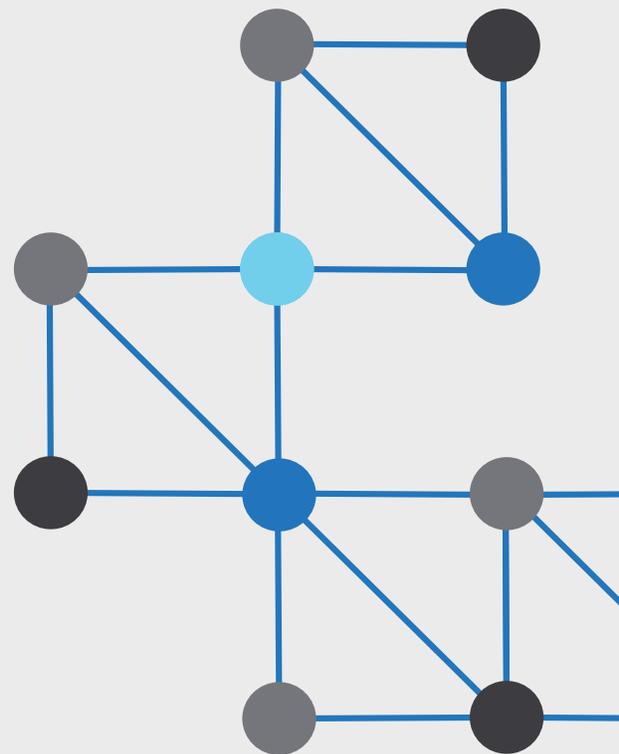
[16] 'Azure Hybrid Benefit'. Microsoft Azure. Accessed November 6, 2019. https://azure.microsoft.com/pricing/hybrid-benefit.

[17] 'Azure Reserved Virtual Machine Instances.' Microsoft Azure. Accessed November 6, 2019. https://azure.microsoft.com/en-us/pricing/reserved -vm-instances.

Organisational change management

Some at organisations initially believe the cloud to be just a 'technical thing'. In fact, as those at companies progress in their adoption of the cloud, they find that the cloud mandates change across many different groups.

For example, as new skills are required, the human resources team may be called in to provide new training opportunities, and career ladders may be adjusted to incentivise mastering cloud skills. New roles (below) will be created as older jobs will decrease in importance.

Account Manager

Solution Architect   ('solve the business problem')

Enterprise Architect   ('urban planner')

Relationship Manager   ('trusted advisor')

Business Architect   ('best use of assets')

Process Engineer   ('real-enough time')

UI Designer — UX Engineer

Scenario Focused Engineering   ('it works')

Tester — SDET

DevOps   ('infrastructure-as-code')

Developer

OPSupport

Statistician/Analyst

Data Scientist   ('business insight')

DBA — Data Analyst

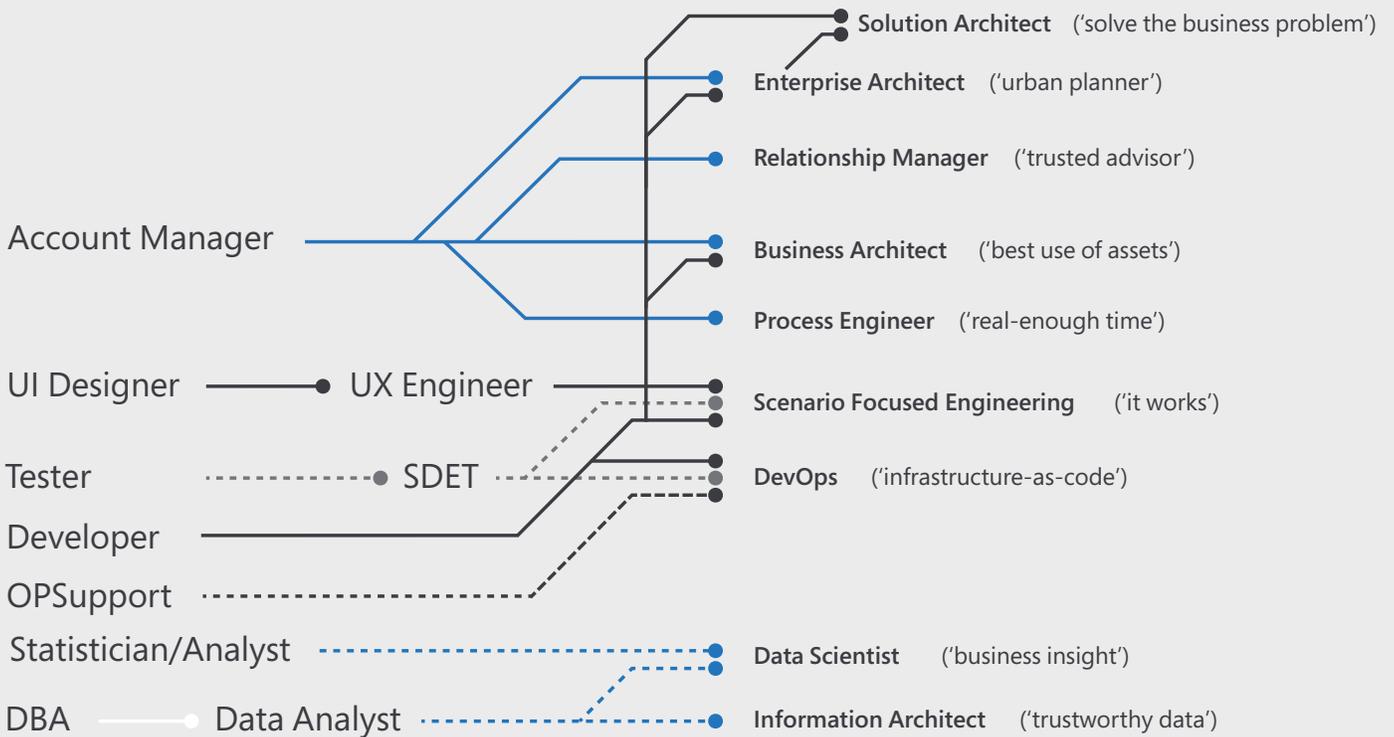Information Architect   ('trustworthy data')

Figure 2-4. Role evolution in the cloud era

Establishing cloud governance

A key function to create in the strategy phase is governance. As your use of the cloud grows, you'll want to maintain control by establishing standards for its usage and monitoring to ensure those standards are adhered to. Examples of such standards include

- which cloud providers is allowed;

- which services are approved (e.g. which relational database(s) is the 'standard');

- cost guidelines;

- adherence to reference architectures;

- architecture reviews; and

- compliance reviews and audits.

Want to learn more about best practices for governance in the cloud? Go to the series of articles starting with

[Governance in the Microsoft Cloud Adoption Framework for Azure](#).

Cloud governance is perhaps one of the most important functions you'll create in the course of finalising your strategy. Governance is an ongoing activity that ensures strategy and its benefits are realised.

How to get started with cloud governance?

Think about your business, IT and organisational goals, as well as your risks; then establish a methodology to help you achieve your end state. Take the time to benchmark your current state relative to your goals and risks, then build your initial governance *foundation*, that is, the initial core set of principles to govern against (e.g. deployment rules to ensure security best practices, cost guidelines, etc.), and then continue to build and iterate.

We'll talk more about governance, and the tools available to you, in Chapter 4.

3. Getting ready for the migration

Now that you've developed your goals and strategy for the cloud, it's time to start executing them. The first step in preparing for the actual migration is to prioritise your application and data portfolio. Which applications should move first – and more importantly, what are the criteria upon which you make that decision?

In the next few paragraphs we'll describe some approaches you can take toward achieving this important step in your cloud journey.
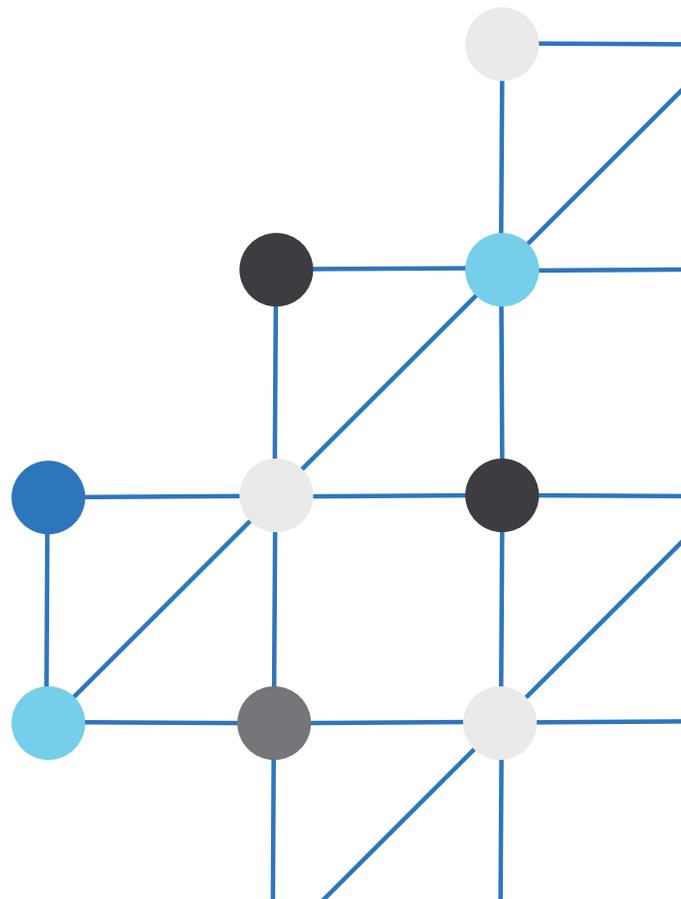
Consider starting with dev/test

Before considering the problem of migrating production applications, look for 'low-hanging fruit' – applications that involve little risk in moving to the cloud. Many organisations following this approach move development and test (dev/test) environments first.

There are a number of good reasons to start here:

- **Dev/test environments are expensive,** and cost savings – sometimes considerable – can be gained by moving them to the cloud. Often, there are three separate environments per application, completely distinct from production: the development environment, the test environment, used by QA to run unit and automated tests and the user acceptance test environment. That can be a lot of servers and VMs that are no longer needed in the datacentre.

- **It's a great way for teams to get familiar with migration tools.** Teams can learn migration tools without affecting the production environment so that when it's time to move production, that migration benefits from the experience gained with dev/test.

- **Developers are generally more tolerant of problems than users are.** In other words, if something goes wrong, production users are not affected, and developers and IT staff can learn from the mistakes.

- **Order matters less.** As we will discuss, moving production applications should follow the prioritisation guidelines. This is less important with dev/test applications – with the caveat that the compliance rules and regulations around protected data such as PII apply whether in dev/test or production (which is why in development anonymised data is often used).

Creating prioritisation rules

As you begin to assess and prioritise your production applications, you have, hopefully, a fair amount of information at your disposal: your application catalogue, your configuration management database and/or the information collected by Azure Migrate or a similar tool. To put these to use, you'll need to develop principles upon which you'll base your prioritisation.

A framework called 'the five R's'[18] can help you begin creating your cloud migration policies. Inspired by a model developed by Gartner in 2011, we've modified it over the years based on our experiences with customer cloud migrations. Here it is:

- **Rehost –** Also known as 'lift and shift', this is a quick way to move applications to the cloud. Properly managed, this approach can reduce costs but does not take full advantage of cloud features.

- **Refactor –** With some rework, an application can be 'refactored' to run in PaaS mode, in which the cloud maintains systems software so that operations teams no longer perform patch and upgrade functions.

- **Rearchitect –** If a legacy application is providing good value but cannot be easily migrated, consider modernising it by rearchitecting for the cloud. Rearchitecting and taking advantage of modern cloud services can make your application more reliable and more scalable.

- **Rebuild –** Consider as well revising the existing application by aggressively adopting advanced cloud services and architectures such as PaaS or SaaS. The process encompasses major revisions to add new functionality or to rearchitect the application for the cloud.

- **Replace –** Often, a legacy application is providing some value, but an off-the-shelf replacement with a lower total cost of ownership is available. Many legacy applications were originally built because there was no alternative at that time. A modern, readily available application that is better suited to running in the cloud – most cost-effectively of all, a SaaS application – may now exist that can be used to replace the older one.

---

[18] Based on 'Gartner Identifies Five Ways to Migrate Applications to the Cloud', Gartner, Inc., 2011. https://www.gartner.com/en/newsroom.

The five R's can be especially useful in quickly identifying applications that can be replaced by SaaS capabilities. For example, consider replacing on-premises email and collaboration applications with Office 365, or an on-premises customer relationship management application with Dynamics 365.

By using SaaS applications (typically charged by the seat), organisations can recoup the costs of servers, licence, maintenance and operations of those applications – and retarget them to new value-add capabilities for the business.
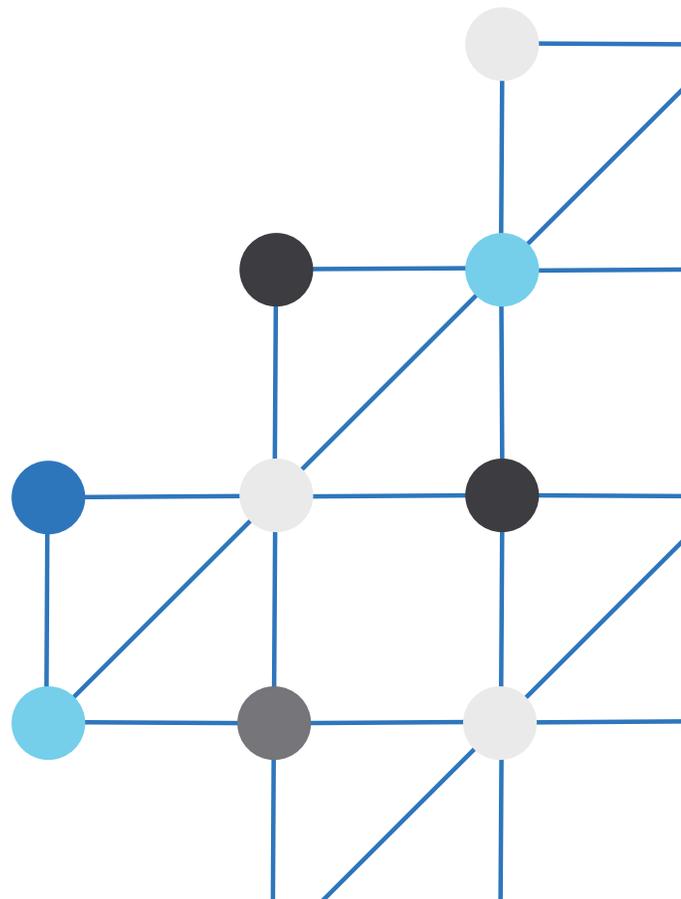
Determine your targets

As you consider the five R's, and survey the landscape of cloud application architectures as we described in Chapter 1, think about the *destination* of your applications as they move to the cloud.

Typically, organisations initially move many, or even most, of their applications to IaaS, that is, VMs in the cloud, because of the

ease of doing so, and because managing them in the cloud is very similar to on-premises – so little retraining is needed.

And as we've discussed, refactoring or rearchitecting applications to be cloud-native can yield a number of benefits – scale, extensibility, reliability, among them. Here's a flow chart describing some of your options:
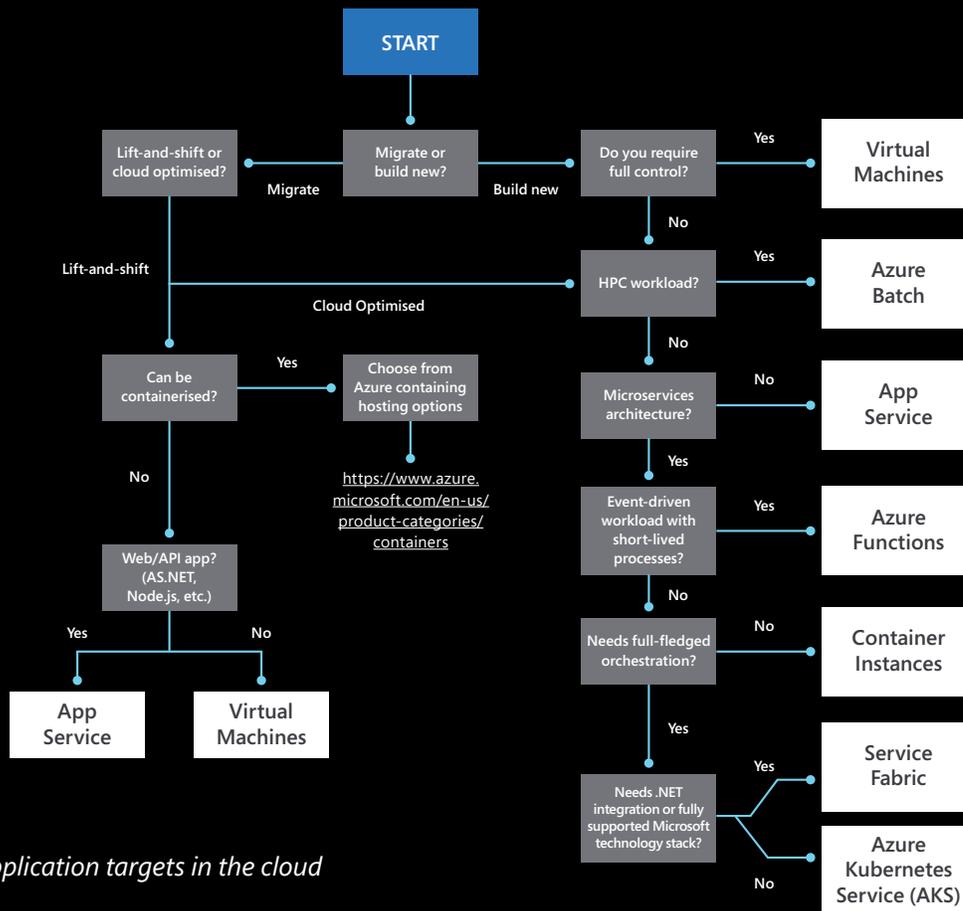
Figure 3-1. Application targets in the cloud

Figure 3-2. Conservative and aggressive approaches

Prioritisation criteria

But which applications should move first?

Here it's worth mentioning that organisations have different philosophies regarding prioritisation.

Most companies begin by identifying low-risk applications and prioritising them first. A few, however, start with a business-critical application – to quickly demonstrate the return on investment of the cloud to stakeholders. Of course, there are many strategies in the middle: which you choose is up to you.

Either way, as you prioritise your estate, consider which criteria to use. Commonly used criteria for prioritisation include:

- **Overall risk,** as we mentioned earlier. Does the application manage business-critical operations or data? Does it have sensitive data whose exposure would be damaging?

- **Anticipated TCO.** With the information gathered, and a knowledge of how to right-size and optimise an application's footprint in the cloud (as we discussed in the previous chapter), you can estimate the total cost of ownership of applications in the cloud.

- **Seasonality.** Are there times of the year when demand spikes and others that are more 'quiet'? If so, you can take advantage of the cloud's elasticity and perhaps save significant costs.

- **Return on investment.** Similarly, an understanding of the TCO can lead you to an estimate of the ROI of the application in the cloud, perhaps taking advantage of cloud features such as scale or cloud services like machine learning. You may wish to prioritise applications whose data can yield new insights by using such services.

- **Integration complexity.** Some applications – ERP is a common example – are 'heavily integrated', meaning that they exchange data with many other applications, often by variety of techniques (ETL, message passing, etc.). Migration in such cases will involve a 'rewiring' effort.

  It's worth pointing out, however, that cloud migration offers an excellent opportunity to evaluate and perhaps transition to cloud-based data exchange tools, such as Azure Data Factory,[19] event-driven serverless functions, and others.

Ultimately, you'll get a view on your application portfolio that allows you to prioritise migration:

Potential Benefits
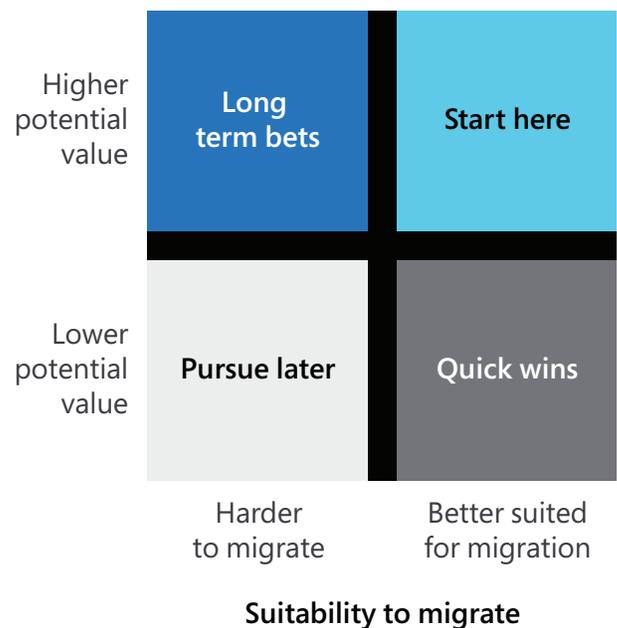
Figure 3-3. Application migration suitability versus potential benefit

[19] 'Data Factory'. Microsoft Azure. Accessed November 6, 2019. https://azure.microsoft.com/services/data-factory.

Develop your cloud data strategy

Of course, migrating your applications is only half the story. You'll also want to consider moving your data to the cloud as well, and here you have a number of decisions to make:

• Do you want to move your database to an IaaS virtual machine in the cloud or to a managed relational database? It's relatively straightforward to 'lift and shift' your on-premises relational database to Azure, but as with IaaS-based applications, you'll still have to manage patches and upgrades yourself.

By taking advantage of a managed relational database such as Azure SQL Database[20] or Azure SQL Database managed instances[21] (more on this later), you'll get elastic scale and reduced management costs while maintaining almost 100% code compatibility.

• Do you want to migrate your on-premises Oracle database to a managed relational database in the cloud? Of course, you can run Oracle in an IaaS VM, but this might be an opportunity to examine the cost efficiencies of moving to a managed SQL Server instance in Azure.

• Can you take advantage of a NoSQL database in Azure? Perhaps you should consider moving some or all of your non-transactional data to a NoSQL database like Azure Cosmos DB.

• And don't forget about your data warehouse. Azure SQL Data Warehouse[22] offers the same pay-as-you-go model for data warehousing as nearly all services in the cloud.

[20] 'Azure SQL Database'. Microsoft Azure. Accessed November 6, 2019. https://azure.microsoft.com/services/sql-database.

[21] 'What is Azure SQL Database managed instance?' November 3, 2019. https://docs.microsoft.com/azure/sql-database/sql-database-managed -instance.

[22] 'Azure Synapse Analytics.' Microsoft Azure. Accessed November 6, 2019. https://azure.microsoft.com/services/synapse-analytics.
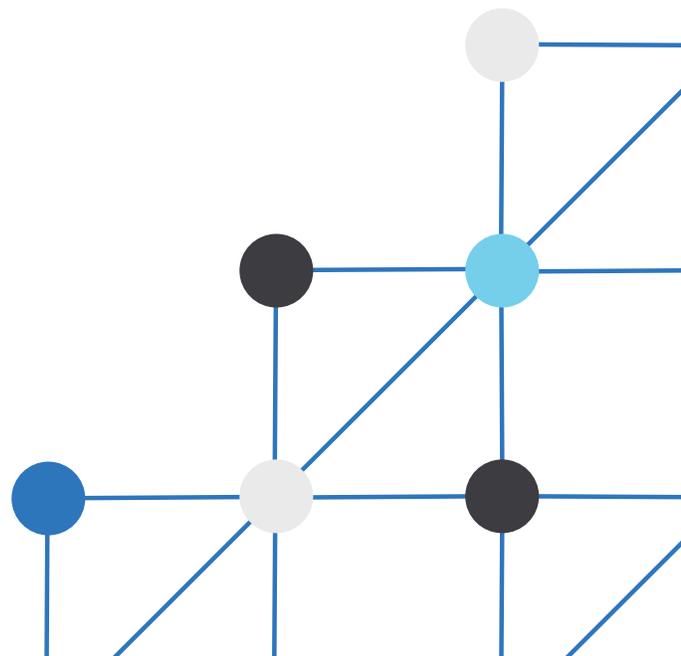
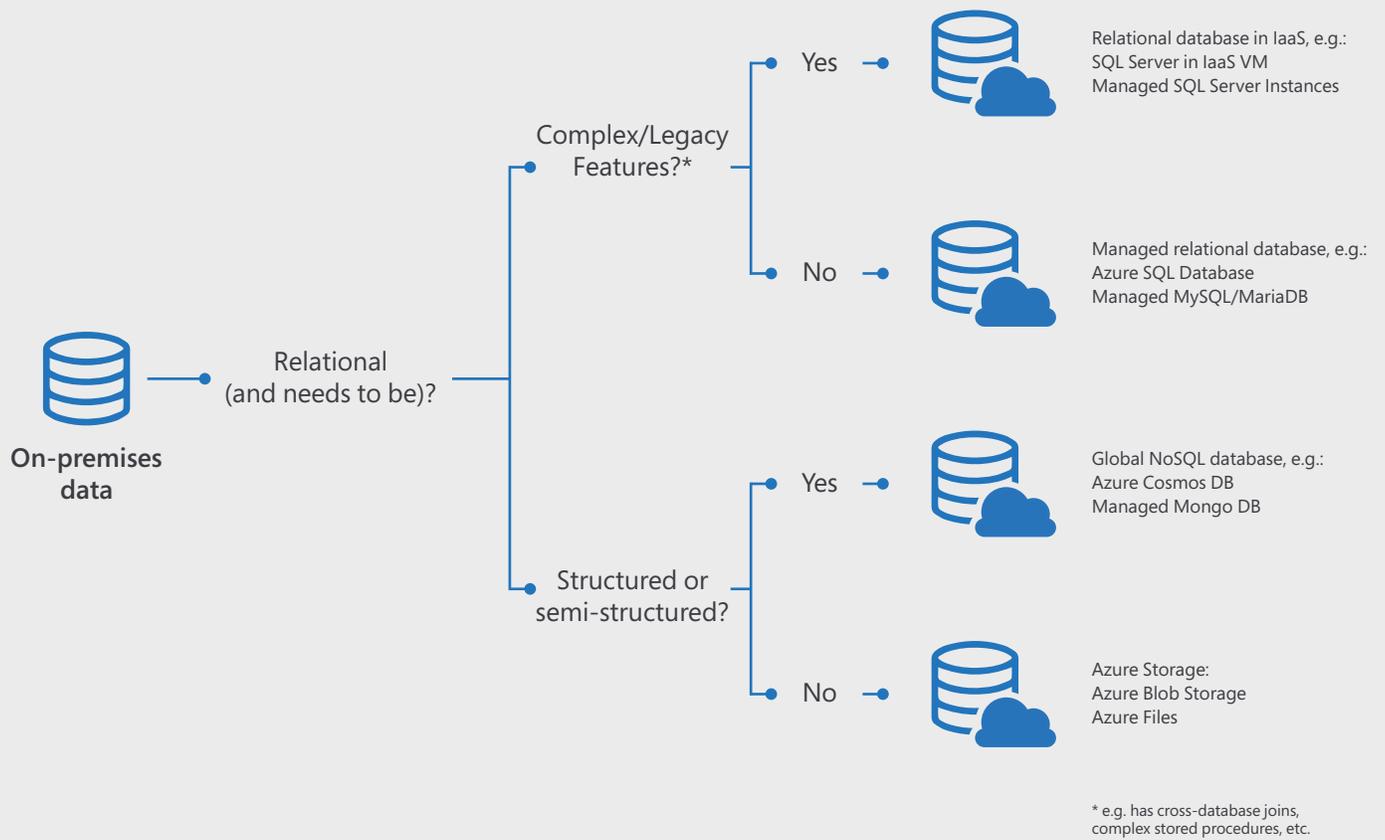# Here's a handy way of summarising the above decision points:

Figure 3-4. Data targets in the cloud

Setting up your cloud infrastructure

In the next few sections we'll talk about some of the decisions you'll face as you begin to set up the core infrastructure for your migration.

The Azure Readiness Guide[23] is a great resource that provides much more detail – and it's a part of the Azure portal as well.

Learn more about
Azure Virtual Networks.
Go to the article:

What is VPN Gateway? →

Networking

Whether you plan to always have some applications on-premises, or instead you set a goal of moving everything to the cloud, there will be a time during which some of your computing estate will be in your datacentre and some in the cloud.

What is the best approach for networking them together to appear as a seamless whole?

Virtual Network

With a virtual network, you can connect your datacentre applications to your cloud applications with full isolation and security; as they share a single IP space, your applications all appear to be locally connected. You can use either IPv4 or IPv6 (at this writing, IPv6 for Azure Virtual Network is in public preview).[24]

With Azure Virtual Networks you can also set up custom security groups (allowing or preventing certain types of traffic to go to specified destinations, for example), routing rules and peering (allowing different Azure Virtual Networks to interoperate).

You can also expose the Azure Virtual Network to application containers and to Kubernetes pods (groups of containers).

[23] 'Azure setup guide: Before you start.' Microsoft Docs, April 8, 2019. https://docs.microsoft.com/azure/cloud-adoption-framework/ready / azure-readiness-guide/index.

[24] 'What is IPv6 for Azure Virtual Network? (Preview).' Microsoft Docs. July 14, 2019. https://docs.microsoft.com/azure/virtual-network/ ipv6 -overview.

ExpressRoute

An alternative mechanism for connecting your datacentre to Azure utilises a dedicated network connection, bypassing the public internet: Azure ExpressRoute.[25]

With Azure ExpressRoute, you directly connect to Azure from your existing WAN network – such as a multiprotocol label switching virtual network, provided by your network service provider.

Using such a dedicated line offers some key advantages. First among them is speed, in the case of ExpressRoute up to 100 Gbps, depending on predetermined charging rates.

In addition, because ExpressRoute does not run over the internet, your connection is private and because traffic is not routed across internet 'hops', latencies can be lower and response times can be more predictable and consistent.

Azure ExpressRoute can also be used with Office 365. For more details, go to the article:

Azure ExpressRoute for Office 365.   →

[25] 'Azure ExpressRoute'. Microsoft Azure. Accessed November 6, 2019. https://azure.microsoft.com/services/expressroute.

Use blueprints to create landing zones

As the last step in readying your ecosystem for migration, create a *migration landing zone*.

A landing zone is an environment that has been configured, provisioned and prepared to host the workloads that you will be migrating from your datacentre.

For example, you set policies to limit which virtual machine sizes can be selected for your applications, easing management and controlling costs. You can also set other limits, such as the number of VMs per subscription, database selections, and so on.

Now, you may wish to have different – but 'standard' – default configurations for different workloads, for example, for dev/test or for compliance-governed applications. To simplify control of these configurations, specifically

meaning Azure Resource Manager templates, role-based access controls and policies, use Azure Blueprints[26] (in public preview at this writing).

Azure Blueprints make it easy for central architecture teams to develop standard, governed and source- controlled configurations for cloud applications, which can then be distributed to applications teams. In addition, Microsoft makes available a number of pre-packaged blueprints that map Azure Policy definitions to specific controls, such as NIST's SP 800-53 (the National Institute of Standards and Technology's security and privacy controls).[27] (For a complete list of Blueprint samples, go here.)

Interested in learning more about using blueprints to create Azure landing zones? Go to the article:

Deploy a migration landing zone.   →

[26] 'Azure Blueprints (Preview).' Microsoft Azure. Accessed November 6, 2019. https://azure.microsoft.com/services/blueprints.

[27] Kim, Lily. 'New Azure Blueprint Simplifies Compliance with NIST SP 800-53.' Microsoft Azure Blog, August 1, 2019. https://azure.microsoft .com/blog/new-azure-blueprint-simplifies-compliance-with-nist -sp-800-53.

4. Adoption: Making the move

It's now time to put into action all the preparations you've made in the past few sections. In this chapter we'll provide an overview of some of the techniques and tools you and your teams can use to move application workloads to Azure.
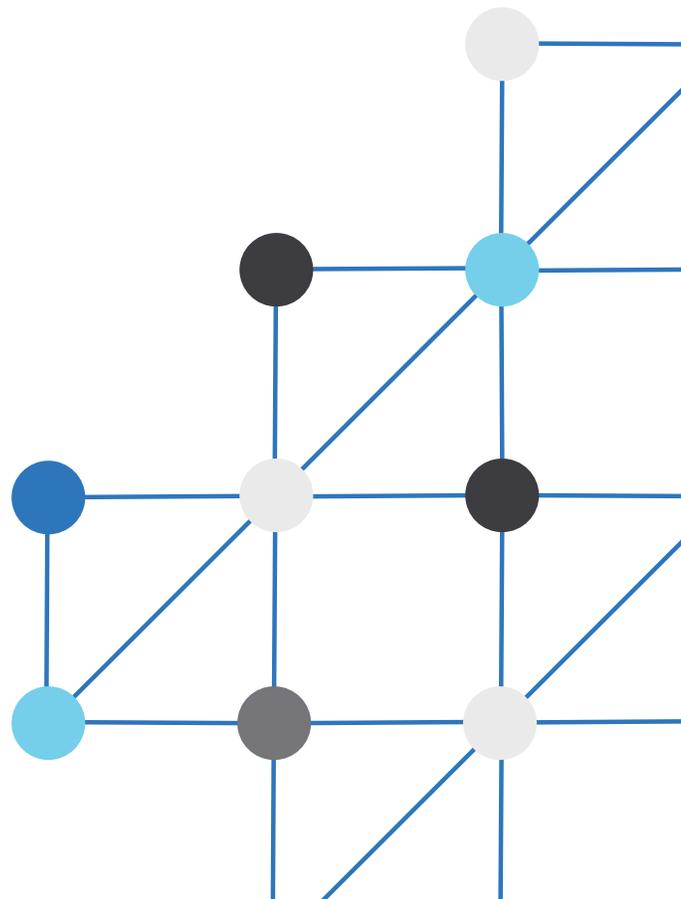
Tools to migrate your applications

The basic idea behind migrating a VM is simple, and can be done from Azure Migrate, from the command line (PowerShell), or via partner tools. In effect, you copy your VM (as a file, for example, as a VHD or VMDK) to Azure Storage and then configure an Azure VM to launch it:

Create and run
Azure VM

Copy VM to Azure Blob
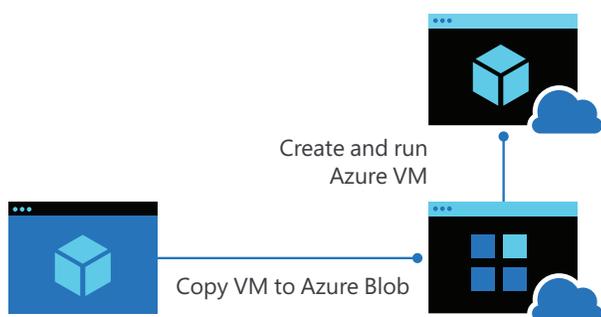
Figure 4-1. Migrating a VM

Of course, you'll have to reconfigure a few things, such as the VM's IP address, routing rules and so forth, to ensure that the cloud VM is visible and accessible to your corporate network.

As we discussed earlier, Azure Migrate[28] provides a centralised hub to assist you with discovery, assessment and migration of infrastructure, applications and data. You can also use Azure Site Recovery[29] to migrate application VMs from one location

For an in-depth walk-through of migration, go to the eBook

[Cloud Migration Essentials: A Guide to Migrating Servers and Virtual Machines.](#)

→

to Azure (e.g. from your datacentre, or from Amazon Web Services). Azure Site Recovery offers additional functionality to set up a business continuity and disaster recovery strategy to ensure your applications are always available. Many Microsoft partners also offer tools to help you with assessing, migrating and optimising your migrations.

Both Azure Migrate and Azure Site Recovery are available through the Azure Portal.[30] For much more detail about running Azure Site Recovery to migrate your applications, read the article: [Migrate on-premises machines to Azure.](#)

---

[28] 'About Azure Migrate.' Microsoft Docs. October 21, 2019. https://docs.microsoft.com/azure/migrate/migrate-services-overview.

[29] 'Azure Site Recovery Documentation.' Microsoft Docs. Accessed November 6, 2019. https://docs.microsoft.com/azure/site-recovery.

[30] Microsoft Azure portal. https://portal.azure.com.

Azure Migrate, as we've mentioned, provides a convenient hub for all the tasks associated with migration; when you log on to the Azure portal, it provides with you with a step-by-step process:

Figure 4-2. Azure Migrate

Most IT ecosystems support large numbers of virtual machines – sometimes tens of thousands – and over time you'll want to understand how to migrate at scale. Azure tools such as Migrate and Site Recovery can help with this task, as well as PowerShell command-line scripts.[31]
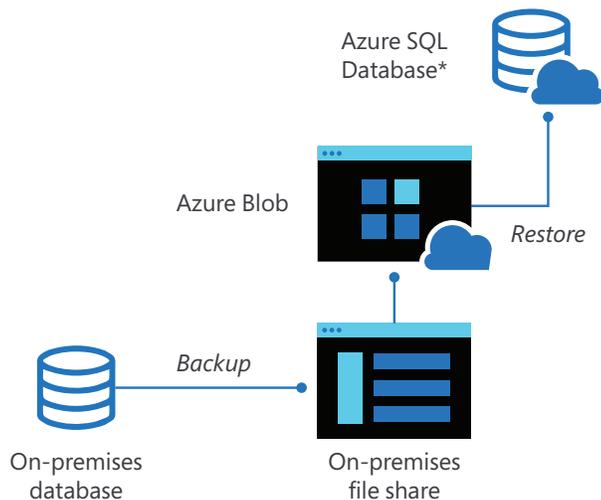
For a demonstration showing how to migrate a database to Azure, go to:

Azure Database Migration Service.

Migrating data

Azure Migrate supports migrating not only your applications, but databases as well, by leveraging the Azure Database Migration Service (DMS).

Migrating databases is a straightforward task. Azure DMS creates a backup file of the database, copies it to a file share on-premises, then copies it to an Azure Blob. Finally, the cloud database restores from the backup in the Azure Blob, as shown in the illustration below (which should look familiar to you from the illustration on VM migration).

Azure SQL Database*

Azure Blob

Restore

Backup

On-premises database

On-premises file share

*or Azure SQL Managed Instance

Figure 4-3. Migrating databases

---

[31] 'Azure/azure-docs-powershell-samples.' GitHub. https://github.com /Azure/azure-docs-powershell-samples/ tree/master/azure-migrate /migrate-at-scale-with-site-recovery.

A note on very large data stores

Typically, companies move on-premises databases to the cloud by using tools that copy the data over a network, either a virtual network or ExpressRoute as we discussed earlier.

However, very large data stores may simply take too long – days, or longer – if moved over a network.

In that case it may be more advantageous to use Azure Data Box,[32] which is a physical device onto which you can copy data and then have transported to an Azure datacentre.

These appliances come in various sizes and are encrypted to ensure safe transit.

[32] 'Azure Data Box'. Microsoft Azure. Accessed November 6, 2019.
https://azure.microsoft.com/services/databox.

Optimising your cloud estate

One of the most important tasks you will perform as you migrate applications to the cloud is to ensure that your cloud footprint is optimised, that is, that your organisation is getting the most for its investment.

It's common, for example, for applications in the datacentre to be *over-provisioned*, that is, applications have more compute capacity than is needed. Why? IT managers wisely want to make sure that their apps can handle spikes in usage and traffic. In the illustration below, for example, eight VMs support a particular application – and monitoring shows that it is largely *idle* most of the year, with CPU utilisation in the single digits.
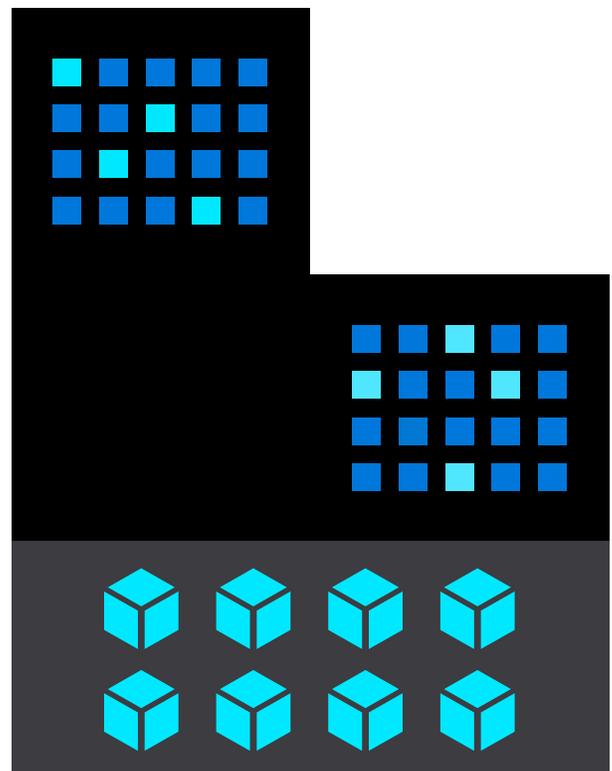

Figure 4-4. Eight VMs supporting an application on-premises

However, it *is* heavily used for a few weeks during the winter holiday season; hence, it's only prudent to have all these instances.

Once deployed in the cloud, you can assign it a minimum number of servers for those idle periods, then scale up as needed – and then back down as traffic subsides, as shown in the illustration below.

Consider also 'right-sizing' your deployment: for those slack times, host your application on smaller servers with fewer cores and less memory. Then, as you approach the periods of peak activity, use more powerful resources: this will result in optimal use of cloud resources – and saving money.
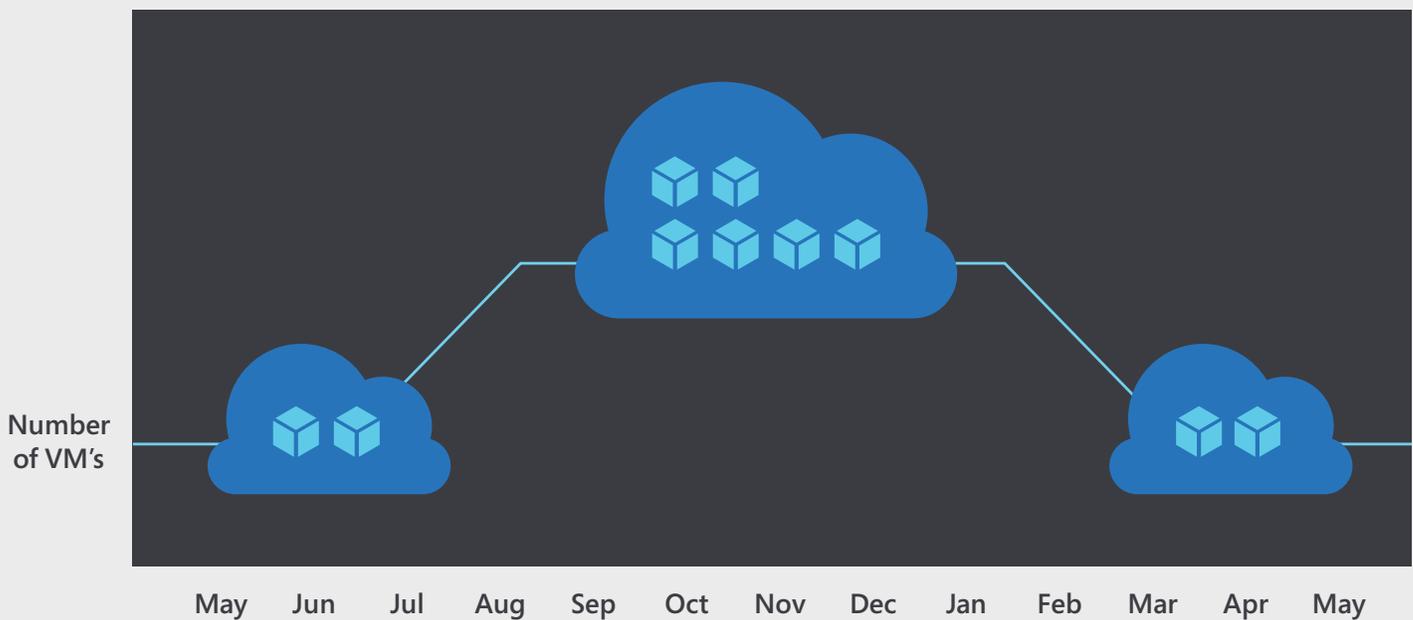

Figure 4-5. In the cloud, the number of resources adjusts to load

Getting the most from your Azure investment

Moving to the cloud is a significant event, and to get the most value from your cloud investment you'll want to establish a solid cloud operations strategy. Many tools exist to help you optimise your cloud applications, not only from Microsoft but also from Microsoft Azure partners.

However, to get the best from your tools, consider your ongoing goals and objectives – above all, to achieve the highest availability, highest business value and highest efficiency from your cloud assets. Enrol your business partners in this effort, to understand their expectations in terms of what functionality is most critical, what their expected KPIs are, what trade-offs (e.g. cost) they're willing to make to achieve these goals and how you will report on them.

Effective cloud operations require focus and attention to detail, and properly designed, can and should be a set of commitments between IT and your business partners.

Cloud operations consist of these five disciplines:

1. **Inventory and visibility**, that is, having a detailed knowledge and visibility into the existence and state of each asset.

2. **Operational compliance**, ensuring that cloud assets are properly sized and configured to achieve the desired performance and reach agreed-upon metrics.

3. **Protection and recovery**, that is, the tools and processes to ensure business continuity and minimising operational interruptions.

4. **Platform operations,** a consistent set of management guidelines and processes for commonly used application platforms (e.g. for Azure SQL, which may have many instances supporting many applications).

5. **Workload operations,** tools and processes to ensure the workload or application as a whole (infrastructure, OS, database, integration, and so on) meets the needs of the business.

In the next few sections, we'll take a brief look at some of the tools you can use to achieve your operational goals.

Monitoring your cloud applications

First, a cloud monitoring application, as the name suggests, monitors the availability and performance of your applications in the cloud.

Azure Monitor collects data from a variety of sources to provide a comprehensive view of both metrics (values at a specific time) and logs (values over time).
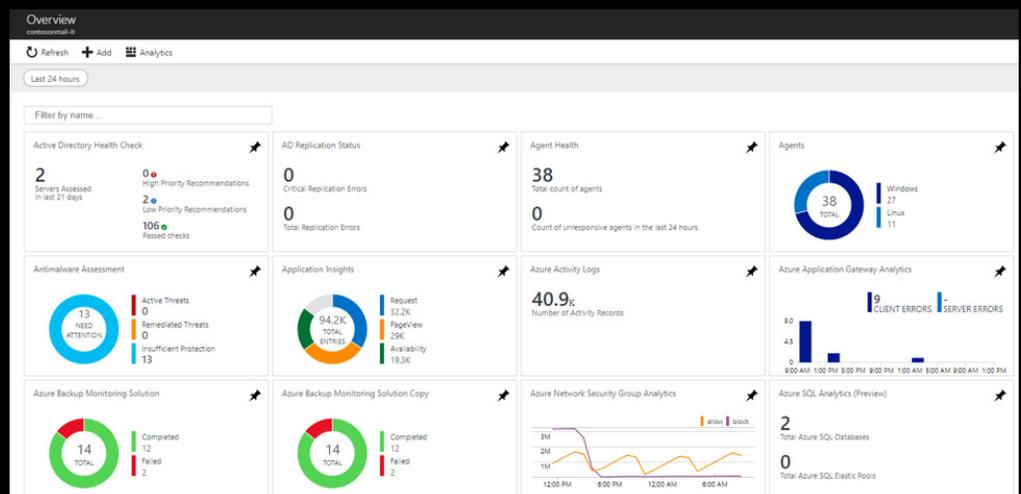

Figure 4-6. Azure Monitor

Good advice from Azure Advisor

With Azure Advisor, a free tool available through the Azure portal, you get recommendations for optimising your cloud deployments customised for you. These recommendations help you ensure

- **high availability** of your cloud applications, by suggesting (where appropriate) the use of availability sets, managed disks and virtual machine redundancy;

- **security,** with a set of recommendations based on an analysis of potential vulnerabilities in your applications based on the latest threat landscape;

- **improved performance,** with a number of suggestions for possible improvements in networking, compute and storage;

- **optimised cost,** by reducing or eliminating unused or underutilised resources in Azure.
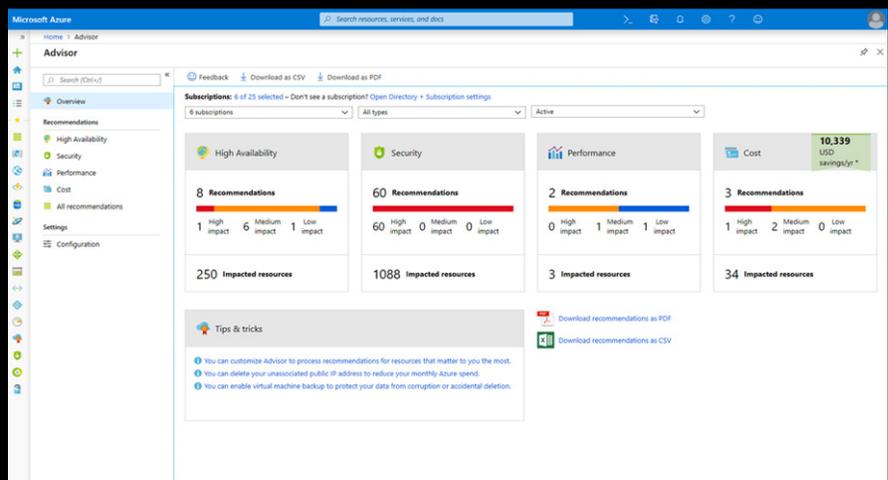

Figure 4-7. Azure Advisor

Managing your costs in the cloud

As we've noted earlier, monitoring costs in the cloud is important, as any number of factors can cause costs to vary from month to month – an unexpected spike in traffic, a misconfiguration, a new team using cloud services, to name a few.

Part of the governance function, of course, is to establish budgets for organisational groups, solutions and/or individual applications.

Azure provides two tools for monitoring costs in the cloud: Azure Cost Management, which is a native tool for creating and managing budgets, reporting and optimising spend; and Cloudyn.[33] Many partner tools also exist that provide these and similar functions.

Azure Cost Management and similar tools allow you to monitor the accumulated costs per month, the daily cloud costs, costs per service and by resource, within certain time windows and a wide variety of other 'slicing and dicing'. You can also set alerts so that you are notified if allowed spend is nearing a given threshold so that you can take appropriate action.

[33] 'Consider Cloudyn.' Microsoft Azure. Accessed November 6, 2019. https://docs.microsoft.com/azure/cost-management/overview-cost-mgt#consider-cloudyn.
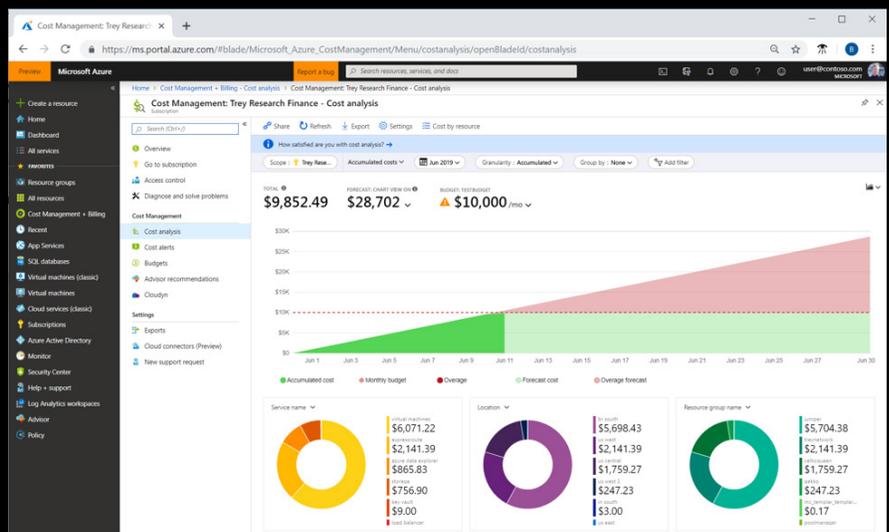

Figure 4-8. Azure Cost Management

Governance

As you operationalise your new cloud estate, it's important that your governance function exercises appropriate control. The 'guardrails' provided by governance help make the growth of the cloud in your organisation more predictable, more reliable and most cost-effective.

As we discussed earlier, use governance to

- **evaluate and monitor costs** to ensure spending guidelines are complied with and that cost accountability is achieved;

- **build a baseline and goals for security** to ensure compliance with IT and regulatory compliance;

- **establish policies for service selection, onboarding and discoverability** to ensure consistency in resource usage;

- **build consistent notions of identity and access** to support security and usage requirements; and

- **use templates, reference architectures and blueprints to accelerate deployment** and achieve consistency and predictability.
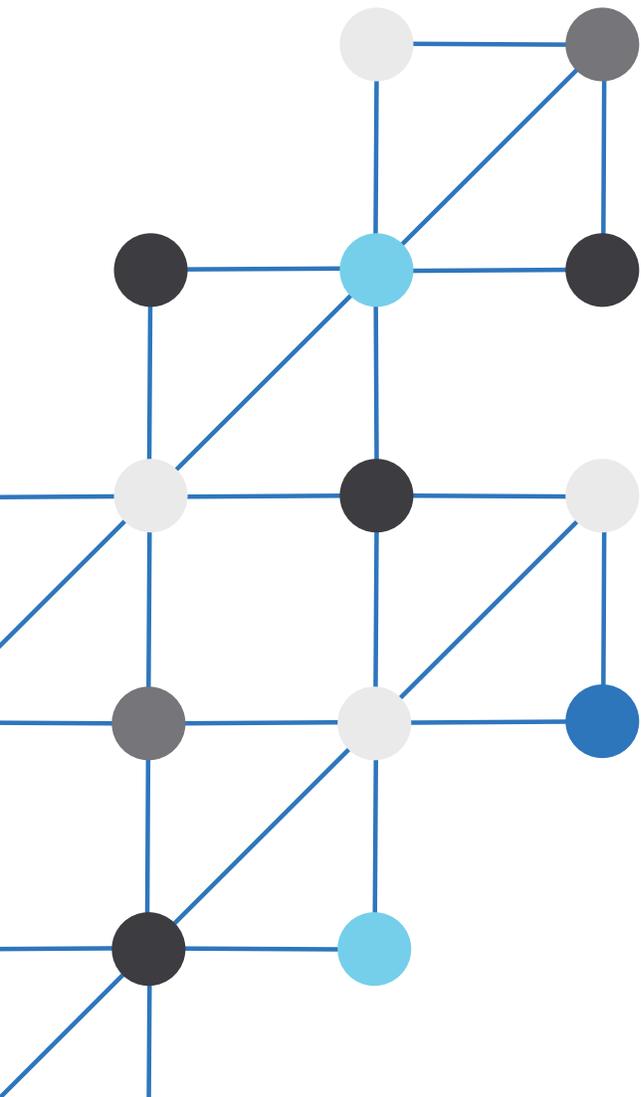
5. Summary and conclusions

In this eBook, we've covered how to think about, plan and execute migration of your applications and data to Microsoft Azure. We started with an overview of the 'why' of the cloud and how your organisation can benefit both in terms of saving money and recouping non-value-add IT costs as well as explore new business models and new ways of doing things.

We then described how you plan your migration. We underscored the importance of describing your goals in the cloud and quantifying them so that you track your progress. We also showed how to catalogue your applications and determine their readiness to be migrated – what we called 'assessing' your IT estate. And, as we mentioned, this is a great time to create your cloud strategy team that will oversee not only the technical but also the financial and organisational aspects of migration.
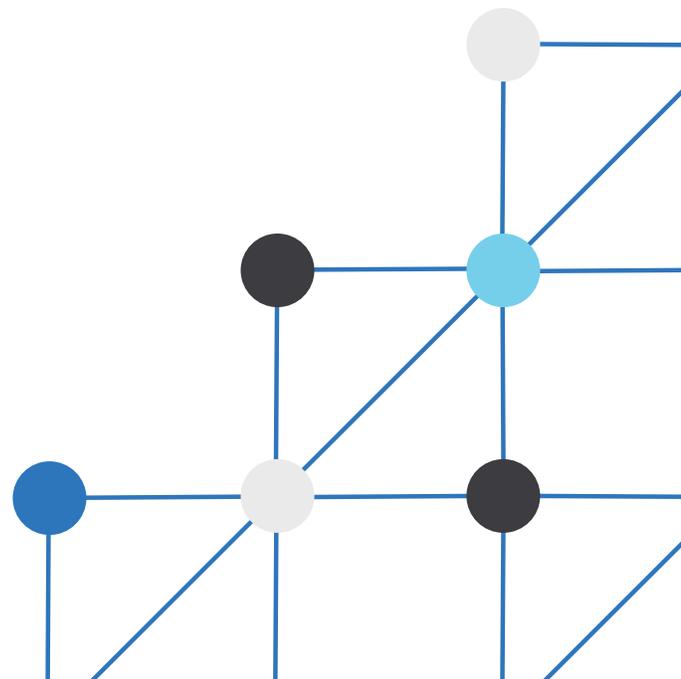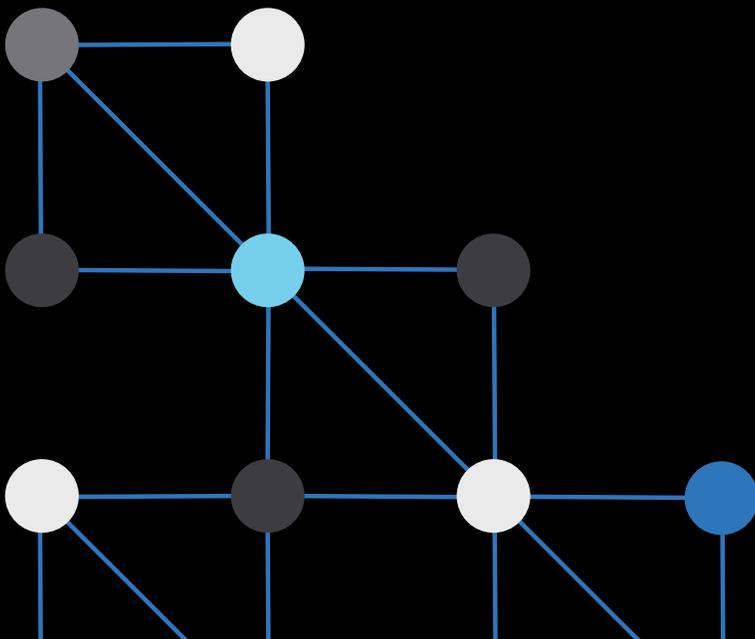
In Chapter 3, we described the next step – getting ready. The 'five R's' – rehost, refactor, rearchitect, rebuild and replace – can help you prioritise your applications. We also described some of the modern 'cloud-native' application architectures that can accelerate getting business value from the cloud. Finally, we discussed the many options you have for migrating your data to the cloud, ranging from managed relational databases to NoSQL databases, each with their own strengths.

Then we talked about the actual migration itself, describing how to use tools like Azure Migrate to move your applications

to the cloud. We also showed a number of tools that can help you optimise your cloud deployments, ensuring you get the most for your cloud investment.

In this overview, we hope that we've helped you better understand the strategies behind cloud migration. Microsoft has a wealth of training, documentation and videos that go into much more detail on each of the topics we've covered, and we've provided links to some in the references section.

For further reading

Azure home page:
https://azure.microsoft.com

Azure documentation home page:
https://docs.microsoft.com/azure

Azure blog:
https://azure.microsoft.com/blog

Azure portal:
https://portal.azure.com

Azure regions:
https://azure.microsoft.com /
global-infrastructure/regions

Azure Trust Centre:
https://www.microsoft.com /
trustcenter/cloudservices/azure

Azure Friday (video series):
https://azure.microsoft.com /
resources/videos/azure-friday

Microsoft Azure channel on YouTube:
https://www.youtube.com/channel/
UC0m -80FnNY2Qb7obvTL_2fA

IDG 2018 Cloud Computing Survey:
https://www.idg.com/tools-for-marketers
/2018-cloud-computing-survey

Cloud Security Alliance:
https://cloudsecurityalliance.org