How to Accelerate Azure Migrations for Financial Services

Planning & Building Compliant Architectures on Azure

Microsoft Partner | Azure Expert MSP

In financial services, mitigating risk is front and center to keep business thriving, customers satisfied, and regulators content. Requirements change, applications evolve, and priorities shift. In this ever-evolving world, where governance, security, compliance, speed, efficiency, and innovation intersect, how can IT teams accelerate migration to the cloud while minimizing disruption to existing governance?

In this eBook, we'll outline concrete steps and real case studies for finance companies that have migrated legacy applications from on-premises to Azure in less than 6 months – often in less than 90 days. We'll show you how to set up a framework that makes migrating legacy applications easier from start to finish without major restructuring of your applications.

Finance on Azure

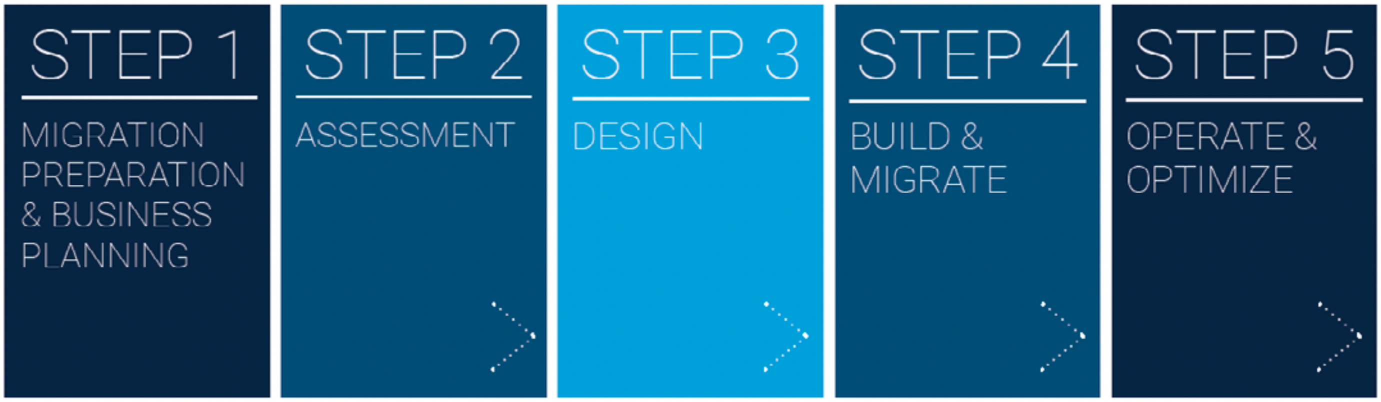
From large financial organizations to FinTech startups, most companies have made significant investments in cloud technology. In fact, 72% of US finance executives say they are either using cloud-based solutions or plan to do so in the future. Many of them have already migrated workloads to the cloud. Nearly 40% of companies are adopting a cloud-first strategy. What's the draw?

Agility and scalability are frequently cited as the top reasons for cloud migration. Long gone are the days when you build an application and run it unchanged for years, and "digital transformation", which often implies a mix of application modernization and cloud adoption, is now a mainstream concept. A cultural shift in favor of customer-obsession and pressure from nimble FinTech startups has pushed the entire finance industry to adopt cloud technologies relatively quickly, despite their risk-averse nature.

Azure has also actively courted financial institutions by strengthening security and governance controls that the industry needs. Azure has achieved nearly every compliance standard a finance organization could want, and there's reason to believe that they hold themselves to a higher standard than many corporate datacenters. Beyond basic encryption, firewall, and logging services, there are now new services like Azure Security Center, a tool that gives you a high-level view of security alerts and compliance status across your Azure and on- premises deployments.

The Migration Process for Finance

Once a financial services company or bank decides that it wants to migrate to Azure, the normal process is as follows:



This process is more or less consistent for any application type. Let's dive into each step more deeply.

1. Migration Preperation

The first step in any migration project is to bring together key stakeholders to discuss and finalize your goals for moving to the cloud.

After helping thousands of organizations move to Azure, the Azure team created the Microsoft Cloud Adoption Framework (CAF) for Azure to provide guidance for each unit in your organization. According to Microsoft, the CAF helps each business unit understand how to update skills, adapt existing processes, and introduce new processes to take maximum advantage of the services provided by cloud computing. The CAF is organized into six steps to help organize your efforts, as seen to the right.

Source: Azure

By breaking down the process into focus areas, each business unit can better plan for the impact of cloud adoption.

The Azure CAF is usually delivered in the format of a live, in-person workshop facilitated by a partner like RapidScale.

Sample Azure CAF Workshop Agenda

The ultimate goal of the Azure Cloud Adoption Framework is to unify stakeholders and create an action plan designed to move your team from cloud goals to cloud implementation.

Governance and the Shared Responsibility Model

For many finance organizations, the "Govern" portion of the Cloud Adoption Framework can be the most challenging area. Governance, Risk, and Compliance teams are unfamiliar with the responsibility model for operating on Azure and often skeptical about security controls they don't directly manage. The most important part of the Discovery and Education phase is educating compliance teams about the Shared Responsibility Model.

By migrating to Azure, you have a shared security responsibility. This shared model means that Azure manages the infrastructure components from the host operating system (virtualization layer) down to the physical security of Microsoft's datacenters. It is your responsibility to configure and secure Azure-provided services. In other words, Microsoft controls physical components; you own and control everything else.

The same line of demarcation applies to IT controls. Customers on Azure shift the management of some IT controls to Azure which results in a shared control environment. Microsoft manages controls associated with the physical and architectural infrastructure deployed in the Azure environment; the customer is responsible for network controls (Security Group configurations), access controls, encryption, and any control not directly managed by Microsoft.

In short, running on Azure is very similar to running your applications in a rented datacenter. You are still responsible for common security operations tasks and for using Azure services in a secure manner.

Common Compliance Task	Insource Azure Management	Outsource Azure Management
Internal Risk Analysis (NIST, SOC2)	Customer	Customer
Internal Risk Analysis: Infrastructure Component	Customer	RapidScale
Attestation of PCI DSS, FFIEC Compliance	Customer	Customer
Attestation of PCI DSS Compliance: Azure Service Configuration Component	Customer	RapidScale
Network Design	Customer	RapidScale
Hardware Provisioning	Azure	Azure
Identity and Access Management	Customer	RapidScale
Image Hardening	Customer	RapidScale
Encryption at Rest	Customer	RapidScale
Logging	Customer	RapidScale
Change Management	Customer	RapidScale
Incident Management	Customer	RapidScale
Tier 1 Support	Customer	RapidScale

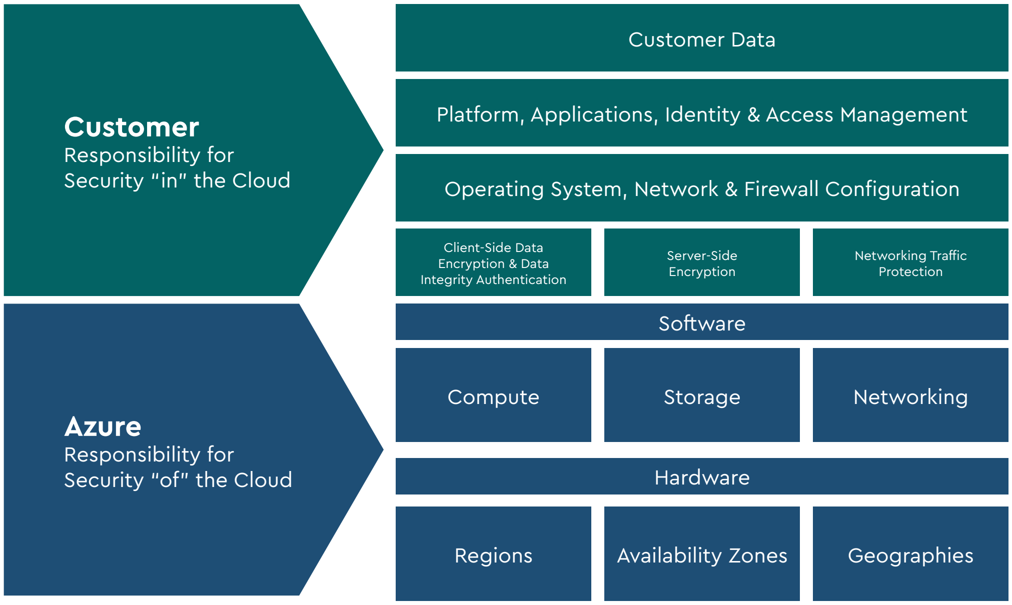
Physical Security and Environmental Controls

If you are concerned about the security of Azure's datacenters, any customer can access a copy of Azure's SOC 2 Type II report, which provides significant detail about physical security and environment controls. This report, ISO 27001, and dozens of others are available for review by audit and compliance teams if you visit Microsoft Service Trust Portal. If an auditor requests specifics regarding the physical controls of your system, they can reference the Microsoft SOC 2 Type II report. Microsoft does not allow datacenter tours, as independent reviews of datacenter security are also part of the SOC, ISO 27001, and other audits.

Data Privacy

Azure customers retain control and ownership of their data, and customers can move data on and off of storage as required. Azure does not leverage any third-party providers to deliver services to customers and therefore does not provide any customer information or access to data to any other provider. Customers must control access to applications and data through the Azure Identity and Access Management service.

Client environments on Azure infrastructure are by default logically segregated from each other and have been designed to prevent customers from accessing instances not assigned to them. Azure has both instances that are dedicated to a single customer (Dedicated Hosts) and instances hosted on shared infrastructure. Azure is responsible for patching the hypervisor and networking services, while customers patch their own guest operating systems, software, and applications.



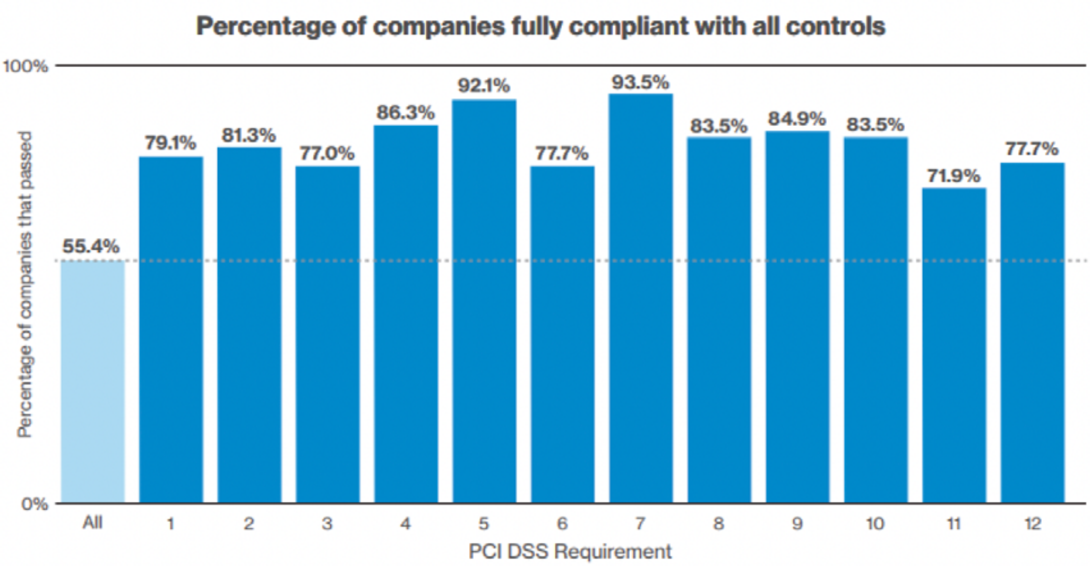
PCI Compliance on Azure

PCI-DSS is usually a baseline security requirement for most finance companies.New Azure customers often ask if Azure is compliant with PCI DSS. The answer is yes. Azure's physical datacenters are PCI DSS Level 1 Certified; however, that does not mean any application running on Azure is PCI compliant. Microsoft provides services that facilitate compliance, but all IT controls above the level of physical infrastructure are a customer's responsibility.

The Payment Card Industry Data Security Standard (PCI DSS) is a security standard that applies to all entities that store, process, or transmit cardholder data or sensitive authentication data. Although the standard was created to protect card payment data, PCI DSS is built on standard security principles, including topics like encryption and access controls that apply to many types of data.

Companies seeking PCI DSS compliance must manage their own compliance certification. If any system with cardholder data or sensitive authentication data is deployed on Azure, your auditor can rely on Azure's Attestation of Compliance for certain physical security controls, but only for services in scope for PCI DSS.

In 2016, only 55.4% of companies met all PCI compliance standards. While this number is up 7% from 2015, it still translates to nearly half of retailers, IT services companies, payment soft- ware providers and hospitality organizations not adequately protecting credit cardholder infor- mation. Additionally, 44.6% of companies fall out of PCI compliance within nine months



Source: Verizon 2017

Companies have the greatest difficulty meeting the following requirements, many of which are related to infrastructure compliance and policies:

- Requirement 3 – Protect stored cardholder data. Requirement 3 also saw the second highest use of compensating controls globally.
- Requirement 6 – Develop and maintain secure systems, covering the security of applications, and particularly change management.
- Requirement 11 – Test security systems and processes, including vulnerability scanning, penetration testing, file integrity monitoring, and intrusion detection.
- Requirement 12 – Maintain information security policies. Control 12.8 ("Manage service providers with whom cardholder data is shared") was the weakest of the Requirement 12 controls.

It is perhaps no great surprise that companies are struggling to meet PCI standards. The vast majority of companies are dramatically increasing their digital footprint at a time when 51% of compliance officers report a skills shortage in compliance.

Companies are expected to meet higher security standards across both legacy IT and cloud-based systems, at a time when IT departments are already stretched, trying to keep up with an accelerated pace of application development.

How to Accelerate the Discovery Phase

For many companies, the Discovery Phase is fairly brief. It can even take place in a single day workshop, or over the course of several weeks. The easiest way to accelerate this process is to get a Consulting Partner to educate each team prior to migration.

But a word of caution: the Discovery Phase is no team should ever bypass. A lot of confusion and rework can be avoided if all members of your team share the same set of goals.

2. Assessment

When tackling a project of significant magnitude, the most challenging part is deciding where to get started. If you already have a project in mind for migration, this step is relatively simple. If your infrastructure is spread across multiple data centers or teams without a unified set of metrics for assessing applications, it can be very difficult to identify the set of applications best suited for the first wave of migration.

Selecting the right applications for migration is both art and science. A combination of the right data and expertise can help you make it through this phase.

Understand and Document Your Current Architecture

In order to identify the right applications for migration, you must have a common method for analyzing, documenting, and evaluating your current infrastructure.

This is where using an architecture assessment solution can help collect and analyze infrastructure performance, usage, and configuration from on-premises or virtualized servers. It funnels data into a single dashboard and can even make recommendations for the cost of running the application on the public cloud.

Using a SaaS tool is far more efficient than asking individual data center teams to inventory application infrastructure, which can take many days or even weeks. Data collected from various teams may be in a different format, making comparisons difficult. A unified, SaaS-based assessment process helps business decision makers compare apples-to-apples in order to make the right migration decisions.

Assessment Category: Reliability

3.1	How are services architected for high availability?	Score
Notes		
3.2	Are there any critical components of your services that are still single points of failure?	Score
Notes		
3.3	Do you monitor for any thresholds indicating availability issues?	Score
Notes		
3.4	Have you experienced any significant service downtime? If so, what was the cause of it and what improvements did you put in place to prevent it in the future?	Score
Notes		
3.5	Have there been performance bottlenecks in any area of your applications (databases, computer, user-interface)?	Score
Notes		
3.6	Are metrics available for traffic, server/app performance, etc?	Score

Example Assessment Workbook that RapidScale uses during initial assessment conversations.

Determine Which Applications to Include in the First Wave of Migration

Once you have collected data on your current systems, it is time to determine the best applications for migration.

There are many criteria to determine the "best" applications to migrate. In Step 1, you should have identified your business priorities and can decide whether you are simply looking for the applications with the greatest cost savings on public cloud or applications whose developers require greater agility.

If you haven't migrated to Azure yet, the best approach is to begin migrating the workloads with the fewest dependencies. This allows you to ramp up slowly, building expertise and confidence before tackling more complex workloads. Another approach is to start with the workloads with the most over-provisioned or idle resources. Industry research suggests that as many as 30% of on-premises servers, both physical and virtual servers, are zombies (showing no signs of useful compute activity for 6 months or more). On top of that, more than 35% of servers showed activity less than 5% of the time. As long as you rightsize your cloud deployment on Azure, these workloads will see the greatest price/performance improvements once migrated.

LOW-HANGING FRUIT WORKLOADS

- Fewest discrepencies
- Over-provisioned servers
- Applications on servers with full capacity

MORE CHALLENGING WORKLOADS

- Large, "tempermental" legacy applications
- Applications that require low-latency connectivity to local fire systems
- Purpose-built appliances like Oracle Exadata and IBM DataPower

Choose a Migration Strategy

Once you've determined your end state and which workloads you will begin with, you must decide on a migration strategy. You may have multiple different strategies depending on the workload, application, and business unit, but organizations typically pick one of the following options:

1. Lift and shift. This approach allows you to keep the application mostly as is while making any necessary adjustments to run on Azure. This is one of the fastest approaches, and there are many migration tools that can assist with the process.
2. Partial refactor. Some aspects of your applications can remain as is, but other parts may need to be rebuilt to operate properly on Azure. A partial refactor may also leave the existing application as is but build additional supporting services on top of it.
3. Full refactor. A full rebuild of your application is the most time-consuming approach, but it also represents the greatest opportunity to take advantage of the elasticity and availability of the Azure Cloud. This could also be a good opportunity to break an application down into microservices or build out a container-based architecture.

4. Transition to SaaS or PaaS. If the workload you are migrating is a commodity application (e.g., email, CRM), or has commodity components (e.g., a relational database), you can incorporate a SaaS or PaaS into the mix. This will help accelerate migration plans as well as reduce management overhead.

A lift and shift strategy is the simplest and fastest approach and is the most common method for companies migrating their first applications to Azure. However, be aware that you may not see significant cost savings. If you use this method, you may not be able to use some of the cost saving services of Azure, like horizontal scaling, managed databases, and more.

How to Accelerate the Assessment Phase

Use an Azure Expert MSP to conduct the assessment and recommend the right cloud platform for you. Unfortunately, many companies get frozen in this step because different teams want different things. A partner can help you get past that phase and move on.

3. Design

The last question to consider is tactical but complex: what will your infrastructure look like on Azure? Which VM types should you use, and in which configurations? How can you maximize your investments?

The ultimate goal of the design phase is to deliver a target reference architecture that is approved by all stakeholders identified in Step 1. This process usually involves the following steps:

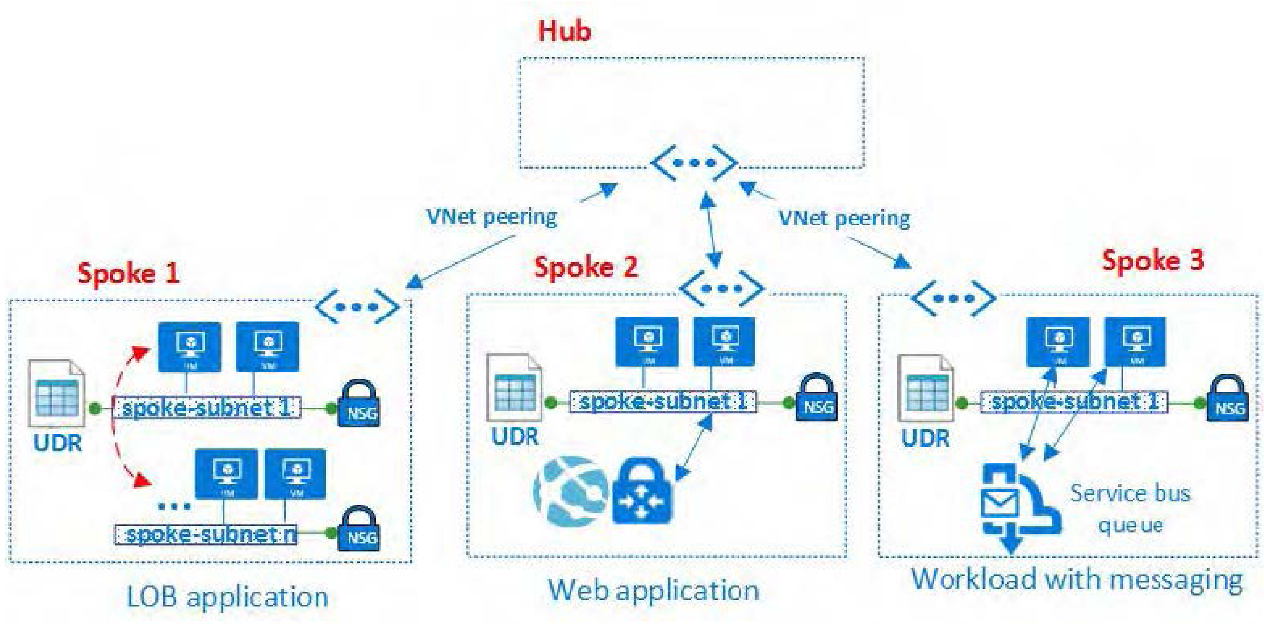
- Look at historical performance data across CPU, memory, network, and disk for servers, and across throughput, capacity, and IO for storage.
- Decide how much "headroom" you want to give each asset (typically 25%), and then look at the actual minimum, maximum, and average usage across these metrics to determine which VM type makes the most sense on Azure. A virtual machine is considered undersized when the amount of CPU demand peaks above 70% for more than 1% of any 1 hour. On the other hand, a virtual machine is considered oversized when the amount of CPU demand is below 30% for more than 1% of the time during a 7-day period. Looking at 30 days of history is sufficient because it is easy to scale up resources on the cloud if needed. When going through this process, it's critical to normalize for different generations of physical infrastructure.
- Design a strawman Azure architecture, both in the form of an architecture diagram and a list of proposed services including VMs, storage, VNs, etc. and associated costs.
- Share with key stakeholders identified in Step 1. If you involve security and compliance teams in the design stage, you will be much more likely to meet your project deadlines than if you involve them after the infrastructure is built out.

The Hub-Spoke VPC Model

Whatever application or workload you're moving to Azure, build your target Azure architecture in a hub-spoke model. This is particularly crucial in any regulated environment.

In a hub-spoke model, several key security features (intrusion detection, logging, bastion hosts, and centralized authentication) should be present in each Virtual Network (VN). Rather than replicating standard features in each VN, you create a central hub VN that is peered to spoke VNs. This provides you with a separation of concerns, network isolation, and a basis for comparison of security groups.

Here's what a standard hub-spoke model might look like on Azure:



Sample Hub-Spoke VPC Model

The Hub VN will contain shared services like the Bastion host, Cisco CSR, Active Directory, and AlertLogic IDS, with VPC Peering between that Hub VPC and Dev, Test, and Prod. It also contains the configuration management master (in this case, Puppet), which is a crucial part of most Azure environments that require compliance.

How to Accelerate the Design + Build Phase

Check out Azure Quickstarts, which are Azure Resource Manager templates designed for specific use cases. With just a few clicks, you can launch infrastructure that Azure has vetted and audited for different compliance frameworks. Here are a few you might be interested in:

- Deploy a simple Windows VM
- Create Storage Account and Blob Container
- Azure Bastion as a Service

If you're starting at square one and don't know how to implement a Resource Manager template, contact a cloud partner.

4. Build & Migrate

The next step is purely technical: your team must build the approved Azure architecture and migrate applications and data to the target architecture.

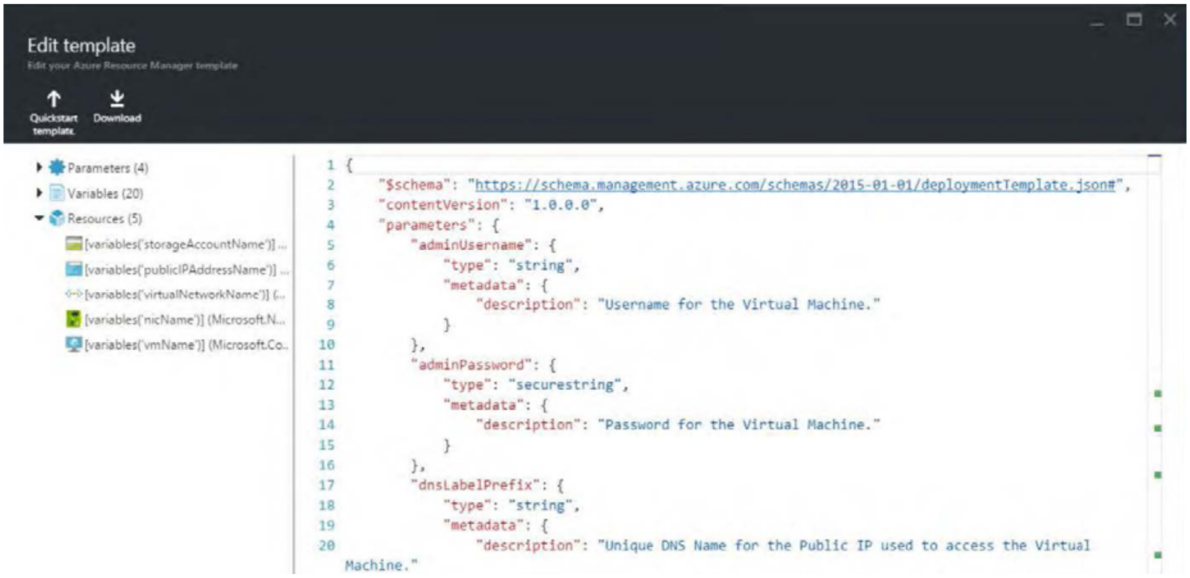
Build Target Azure Architecture

Ideally, the process follows this pattern:

1. Cloud engineers build the approved architecture in Azure Resource Manager, an architecture templating tool that allows you to "build" once and spin out future environments instantly.
2. An Azure-provided machine image is used and further configured for each application using an automated configuration management tool like Puppet or Chef
3. Together, the template and the Puppet or Chef scripts are kept in a code repository (Git) and versioned and updated like a piece of software
4. Servers, databases, and data are migrated to Azure, either over the internet (which takes quite a bit of time), or through an Azure migration service, like those listed below
5. Cloud engineers begin initial testing process where infrastructure is torn down / rebuilt with Azure Resource Manager and configuration management countless times
6. Other teams test and validate application performance, security, compliance, etc.

Many teams make the mistake of building Azure resources manually using the CLI or console. While this may be a quick, short-term solution, it makes the build-out of future test/ dev environments complicated and causes long-term management issues, highlighted below.

When you automate infrastructure build-out from Day 1, you enable your team to build consistent, documented, easily-updated Azure environments. All mature Azure users build and maintain Azure resources with a templating tool like Azure Resource Manager or another tool like Terraform.



Sample Azure Resource Manager template.

Configuration Management

The fundamental purpose of configuration management is to deploy environments prescriptively. By defining everything on the servers in a single location, there is a single source of truth about the state of the entire infrastructure. The value of configuration management is that when you want to change the OS, you can change the code on the servers without making major changes to the servers themselves. Configuration management is also used to install various security features on a VM, like Identity Detection System agents, log shipping, monitoring software, as well as requiring MFA and binding the VM to central authentication. Changes can be rolled out to many instances at once — and be rolled back. When you are done, each server is in a known, ideal state. When you build and maintain your environment manually, change is slow, cannot be rolled back, and has a higher risk of human error.

With Azure, there are many possible tools to control configurations. You can choose to use an Azure native tool like Azure Policy. You can deploy your own server with Puppet, Chef, or another CM tool of your choice. Obviously, the latter provides greater control but requires that you provision and maintain your own Puppet/Chef server.

Migrate Data

After you build your target environment, it is time to move your applications and data. Azure has nearly a dozen services to help you migrate to Azure. Here are just a few examples:

Azure Database Migration Service helps you migrate databases to Azure easily and securely. The source database remains fully operational during the migration, minimizing downtime to applications that rely on the database. The Azure Database Migration Service can migrate your data to and from most widely used commercial and open-source databases.

Azure VMware Solution makes it easy for customers to run VMware workloads on the Azure Cloud. Customers can use VMware's virtualization and management software to seamlessly deploy and manage VMware workloads across all of their on-premise and Azure environments. This will allow customers to leverage existing investments in VMware skill sets and tooling to quickly and seamlessly take advantage of the flexibility and economics of the Azure Cloud.

Azure Migrate is a central hub for starting, executing, and tracking your Azure migration. It allows you to integrate Azure native and ISV tools, organize migration paths, replicate on-premises machines on Azure, and assess the process to uncover issues.

How to Accelerate the Build & Migrate Process

During the migration process, there is a period of time where both your current and your Azure infrastructure will be up and running. This is usually results in higher costs. You should anticipate and budget for this period. The planning done in Steps 1–3 will help minimize the length and impact of this "double" infrastructure period.

That said, this process can last for months or years. At RapidScale, we've seen a company's lack of internal organization translate into migration projects that never get off the ground.

If your migration process is stalled, it could be that you're trying to accomplish too much at once. Go back to the drawing board and launch a POC for your most basic application. Or think about launching a multi-account architecture – where each team or project has a different account and teams' competing priorities won't prevent others from moving forward.

5. Operate & Optimize

While many of the key elements of a cost efficient migration are determined during the migration process, the key to long-term success on Azure is ongoing optimization.

By necessity, you will have some inefficiencies during the migration stage. As environments are tested and instances are changed to meet the demands of the application, there will be unexpected costs. After migration, you will have time to examine those inefficiencies and continually improve your infrastructure.

24/7/365 Ticket Support

During the Business Planning phase, you should have identified the key teams that will manage the Azure environment(s) on an ongoing basis. If you are managing internally, use the time after migration and before go-live to determine SLAs, establish roles and responsibilities, and prepare procedures for common tasks, such as VM rebooting, access management, etc. Relying on an external Managed Services Provider can help reduce the burden of around-the- clock management on internal teams.

Cost Tracking and Analysis

One of the greatest benefits of using Azure cloud is that you can get real-time billing information and notifications of unusual or unexpected spending. In order to filter that information and turn data points into actionable information, use a cost analysis and cloud governance platform. Your cost tracking and analysis dashboard should be your "single pane of glass" over both on-premises and cloud-based environments. Ideally, it should also be accessible by your cloud engineering team, who should be held accountable for maintaining their project budgets. Your team should schedule regular internal reviews related to the cost of the environment. Azure is continually adding new products and services, and these can impact the cost of an environment without the proper guardrails in place. For example, a new VM type that better fits your application may mean you can downsize and save.

Regular Engineering Reviews

Every team should conduct regular engineering reviews every six months. At RapidScale, we use the Well-Architected Framework as a structured approach for evaluating cloud environments based on these five pillars:

- Security
- Reliability
- Performance efficiency
- Cost optimization
- Operational excellence

Regular, formal assessments allow you to have a consistent approach for continuous improvement of your infrastructure and a common standard of excellence across all teams and Azure accounts. Whether you perform these internally or with the help of an approved Azure Gold Partner, these reviews will help lower the ongoing risk of operations, improve cost- efficiency, and expose areas of potential weakness in your architecture.

While a formal review takes place every six months, your team should be constantly measuring your environment against the best practices outlined in the Well-Architected Framework. A SaaS-based governance solution can provide the data and recommendations to keep your team in line with best practices all year long.

Conclusion

Finance companies are increasingly migrating applications to Azure and want to be confident that security and compliance needs are addressed during the process. Compared to non-regulated workloads, regulated workloads will take longer to migrate, mostly due to the extra time required in the Assessment and Design phases. But you can still accelerate migration with the tips described in this eBook.

If you're ready to take the next steps in planning your migration, find out how RapidScale can help simplify the process of migrating assets from your data center to the Azure cloud. RapidScale's Migration Services enable you to efficiently assess and model workloads for migration. Then you can manage and optimize your infrastructure for cost, usage, performance, and security once they are running on the cloud. This helps reduce complexity and allows you to move faster in your migration process. Learn more about how RapidScale can help you plan, build, and manage your cloud environment by visiting www.rapidscale.com.

About RapidScale

RapidScale, the leader in compliant cloud solutions, provides end-to-end cloud strategy, RapidScale helps customers migrate, run, and operate mission-critical workloads on Azure with security, scalability, and efficiency baked in. RapidScale's Cloud Reliability Platform combines world-class engineering talent, policy-as-code, and integrated tooling to enable customers to confidently meet compliance regulations, security requirements, cost control, and high availability. Together with our team of dedicated certified engineers and decades of IT management experience, we ensure our customers' success across every stage of the Cloud Adoption Framework and governance.

Microsoft Partner

Azure Expert MSP

Microsoft