Microsoft Azure

intel.

Modernise Your Business-Critical Systems and Applications with the Cloud

Table of contents

01

Introduction

The term “business modernisation” has become a buzzword in corporate planning discussions; its meaning is often diluted and ambiguous. However, business modernisation simply refers to the modernisation of the applications and systems that companies depend on for day-to-day operations; the essential ones are considered “mission-critical” or “business-critical” systems. While the definitions may vary by company, the need for these systems to be reliable, fast, accessible and secure is universal.

Every organisation has its own definition and parameters for business criticality. For the purposes of this eBook, we adopt the prevailing industry definition that business-critical systems and applications are usually those that are supporting a company’s most important business processes. These are often the systems that, if disrupted, could negatively affect revenues, reputation and customer experiences. As a result, business-critical systems often require the highest service-level agreements for a specific organisation.

Many companies have been transitioning or are planning to transition business-critical workloads to public cloud infrastructure, intensifying the focus on cloud transformation beyond initial proofs of concept, backup, development and testing of workloads. Questions arise on how to stratify business criticality; the tradeoffs between availability and business continuity, resilience, performance, cost and complexity need to be discovered, documented and ultimately governed. Regulated and public sector organisations must consistently consider additional factors as well.

Our conversations with IT executives corroborate the fact that managing business-critical infrastructure on-premises can be quite challenging. In fact, organisations that have migrated their business-critical systems to the cloud report increased ability to meet security and compliance requirements. They cite faster infrastructure deployment times and greater scalability combined with improved operational agility. Nonetheless, customers need proven and reliable migration approaches. Microsoft and its partnerships in regions all over the world have led and supported thousands of successful migrations and data centre consolidations and exits in the past decade. Our experience in business-critical workloads allows us to create and refine a migration approach tailored to the specific needs and priorities of your organisation.

The first half of this eBook shows how to clarify, quantify and distinguish business-critical systems. The second half dives deeper into the steps and technology considerations of an example scenario focused on SAP applications. It provides key learnings and insights for understanding the requirements, risks and alternative approaches of moving your business-critical systems to the cloud.

02

Defining "business-critical"

Customers typically evaluate several criteria to define the business criticality associated with an application or a system. These are the most common we see our customers use:

1. **Service-level agreements (SLAs) or other availability targets:** Business-critical systems and applications are usually those that are the highest SLA for a specific organisation, usually expressed as a percentage. An SLA of 99.99% has a cumulative downtime of 4.32 minutes per month, or 52.56 minutes per year.

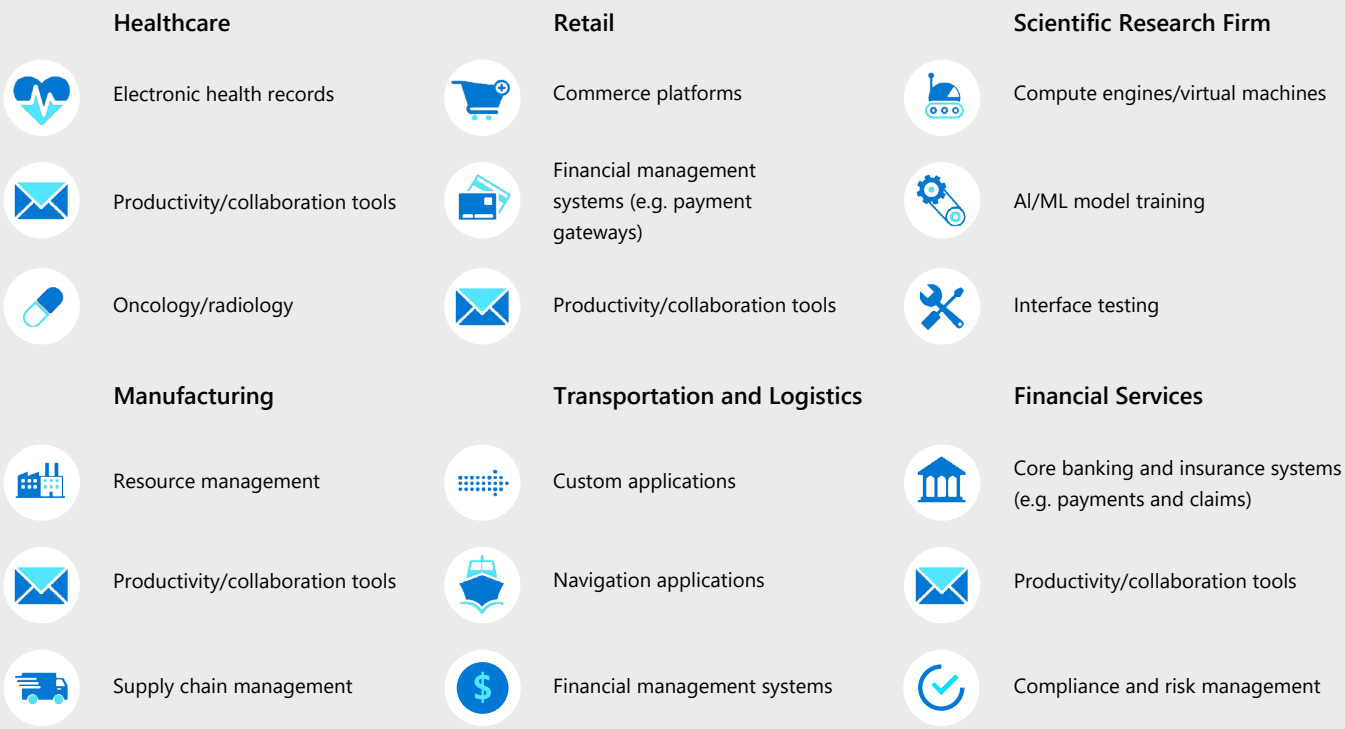
2. **Industry-specific targets:** The type of systems most often classified as business-critical are those customer-facing applications on which an organisation's customers depend to conduct business and transact. Further, we might add middle-office and back-office systems responsible for financial management; governance, risk management and compliance (GRC); and productivity and collaboration (including email and communications tools).

3. **Loss of reputation or trust:** The most important business systems are at the core of a company's critical processes – the ones that cost the most when down or lost and that would have the greatest impact on reputation if there were a security breach.

When planning to move their applications to the cloud, most IT professionals assume that the cloud platform automatically handles most of the reliability and disaster-recovery capabilities. But the cloud model relies on shared responsibility between the cloud provider and the customer. Therefore, there are certain SLAs provided by the vendor to support your application, but the resiliency of the application is the responsibility of the application owner.

While the definitions of "business-critical" may vary, the term simply refers to a system at the core of a business that requires the necessary safeguards and design considerations to help ensure it remains resilient, scalable, maintainable and, to a certain extent, "future-proof."

The diagram below illustrates a few examples of typical business-critical workloads by industry:



Base: Online survey of 412 global enterprise decision makers and six in-depth phone interviews with senior IT leaders
Source: The Move Is On: Modernize Mission-Critical Systems with Cloud, a commissioned study conducted by Forrester Consulting on behalf of Microsoft, March 2020

Figure 1. *Business-critical applications by industry*

Identifying business-critical applications

In our customer conversations, Microsoft uses the following framework to inventory and prioritise on applications. It is meant to align business and IT, and to surface application context that is important in planning the cloud adoption journey.

The framework is meant to be used top to bottom. First, review applications by type and distinguish between native Microsoft applications (e.g., .NET applications), commercial off-the-shelf and other solutions and platforms. Second, and the main topic of this white paper, identify the business criticality of the applications being reviewed. And third, but certainly not less important, is an initial assessment of risk and complexity.

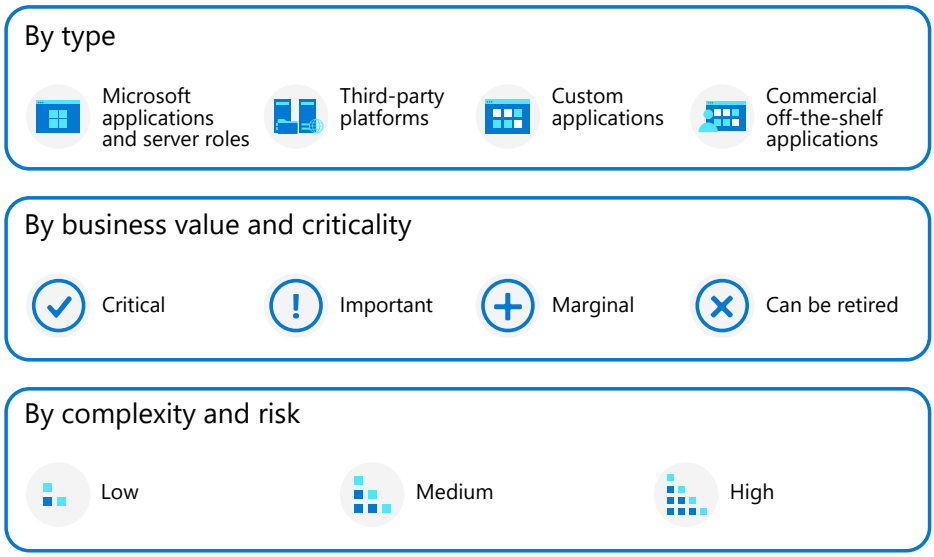


Figure 2. *Framework for assessing your portfolio*

03

Cloud migration: Challenges and benefits

Cloud computing offers elasticity, multiregional expansion, faster deployments and management of infrastructure through infrastructure as code, which provides ease and proven economic benefits. And at this point, no workload is out of scope, including legacy applications. Many organisations are taking a "cloud-first" approach, while factoring in an increasing range of hybrid, multicloud and edge solutions. However, the worry of possible failure can linger.

At times, customers are concerned about the fact that cloud service providers control the infrastructure layer, while cloud consumers lack any control over physical resources. Additionally, compliance adherence and potential security vulnerabilities with new cloud services remain concerns for any customers interested in bringing their business-critical and data-sensitive workloads to the cloud.

For example, sharing a network under multitenancy (i.e., sharing workloads with other tenants), data loss and leakage, physical co-locality, quality of service and resource quotas are a few of the primary concerns associated with the migration of business-critical applications to the cloud.

Other challenges during the cloud migration phase include moving very large amounts of data and multiregional hosting. What follows are insights on the common risks mentioned above and ways to mitigate them.

Fine-grain security and compliance controls

Threat techniques are ever-changing. Cyberattacks appear in new forms including the use of botnets to control networks, cloud-powered attack tactics and the employment of ransomware as a service. An application must be built secure in the default architecture with a security model that is effective for current and future needs such as mobile workforces,

devices, applications and data access. Adopting a Microsoft security framework like the Zero Trust model (i.e., never trust, always verify) can be an effective tool in addressing any threats. The guiding principles of Zero Trust are compliance resource policies, management groups, multifactor authentication, the use of least privileged access, just-in-time access, assuming breach and reducing the blasting radius to minimise the impact. Azure management groups and policy initiatives provide granular compliance controls for reporting or hardening the access to Azure subscriptions. Finally, Active Directory integrations, encryption (with Microsoft or customer-managed keys), enabling Private Link and multiregion replication features can conveniently reduce risk for the platform.

Multicloud

We define "multicloud" here as the purposeful use of platform as a service (PaaS), infrastructure as a service (IaaS) and software as a service (SaaS) from multiple cloud providers. These services are typically a combination of public, edge and hybrid cloud deployment models. There certainly appear to be tradeoffs to this approach and therefore should be carefully evaluated. For instance, on the one hand, many may benefit from the flexibility and best-of-breed capabilities of a multicloud solution. On the other hand, the increased complexity and costs due to the need for multiple skill sets for implementation and support, such as in maintaining multiple automation frameworks across platforms, are clear drawbacks. This may further complicate your DevOps capabilities. Consider your specific business-critical use cases and evaluate complexity versus flexibility related to management and governance, integration, data dispersion and skills requirements.

Leveraging the scale and elasticity of the cloud provider

For business-critical applications, organisations expect the ecosystem to provide control, visibility, elasticity and scalability. Azure as a cloud provider delivers tool sets like infrastructure or application-level monitoring, identity threat protection and services like virtual machine scale sets to rapidly deploy scale-out and highly available applications, storage accounts and app services. Webhooks, functions and desired state configuration types of service can provide fast reaction times for the elasticity or scalability of the solution on the cloud. Introducing minimal modernisation to the applications on Azure (for example, using Azure file share instead of the traditional on-premises file servers) is another way to achieve scalability.

Cloud provider resource availability with respect to critical objectives

If a regional failure occurs, securing adequate cloud resources is one of the most critical tasks. Identifying and mapping the SLA of PaaS, IaaS, domain name system, secret store and database services are essential components in a disaster-recovery scenario. A business-critical application design must address these challenges and provide the necessary risk mitigation. If planned properly, disaster-recovery testing with the application hosted in the cloud provides convenience and proximity to the production failover by using services such as Azure Site Recovery for IaaS, built-in replication systems of PaaS and storage replication to the paired region. Alternatively, you can use cloud automation and DevOps tooling and processes to automatically recover the Azure infrastructure; this way, the application can fail over to the newly launched Azure infrastructure service. Or you can use on-demand capacity reservations to obtain and lock in your compute capacity needs, as you scale up and down your business-critical infrastructure or execute software updates and deployments.

Predicting behaviours

Quality of service for applications deployed on the cloud can be different for applications deployed on-premises where the endpoints are accessed by the next network hop. Predicting behaviour and continuous forecasting can aid in avoiding dips in application quality of service. Consider merging, connecting, monitoring and forecasting solutions with cloud services. Early detection of application performance or quality errors helps in the decision matrix to scale up or down application components.

Cost of running critical applications on the cloud

Application hosting on the cloud can be expensive over time if effective controls are not in place. Forecasting years one through five helps in understanding the expenditures of application resource consumption. In such scenarios, evaluating hosting techniques, such as standard deployment versus bursting with scale sets, or containers for types of services, can solve cost problems by taking advantage of the pay-as-you-go model for the cloud. Reserving compute capacity instances based on forecasted usage, third party versus cloud provider for native solutions, hot versus cold infrastructure for paired regions or controlling resource deployment through governing policy are a few ways to control and spend effectively for business-critical applications.

04

Business criticality: Key tenets

Businesses today require a unification of people, processes and technologies, which need to work together to provide effective solutions and outcomes for customers. For a business system to provide value, it needs to be reliable and as optimal as possible to deliver cost savings while providing tangible benefit. The Azure cloud platform provides a resilient foundation built on world-class global infrastructure. This foundation can be further expanded with additional resiliency features based on the business criticality of your systems.

This section provides an overview. Please consult Microsoft or one of our certified partners if you would like to learn more about the topics discussed below. Beyond this initial overview, please refer to the appendix, specifically the Well-Architected Framework, which covers these guiding tenets in more detail.

The key principles that businesses look for in business-critical cloud platforms are:

- Governance and corporate policy
- Resilience, business continuity and disaster recovery
- Performance
- Reliability
- Security
- Cost optimisation and operational agility

Governance and corporate policy

Corporate policies drive cloud governance. The Cloud Adoption Framework (CAF) governance guide focuses on specific aspects of corporate policy:

Business risks: Identifying and understanding corporate risks.

- Document evolving business risks and the business tolerance for risk, based on data classification and application criticality.

Policy and compliance: Converting risks into policy statements that support any compliance requirements.

- Convert risk decisions into policy statements to establish cloud adoption boundaries.
- Consider and incorporate regulatory requirements.

Processes: Establish processes to monitor violations and ensure adherence to the stated policies.

Resilience, business continuity and disaster recovery

For effective business continuity and disaster recovery, your organisation or enterprise needs to design suitable, platform-level capabilities that application workloads can consume to meet their requirements. Specifically, these application workloads have requirements related to the recovery time objective (RTO) and recovery point objective (RPO). To design capabilities appropriately for these workloads, ensure that you capture your disaster-recovery (DR) requirements.

Critical resilience capabilities can be achieved through a variety of Azure services including availability zones, availability sets, Azure Traffic Manager, Azure Site Recovery, Azure Backup and Azure Storage.

Performance

Virtual machine performance: The performance of your business-critical systems can directly affect customer satisfaction levels, customer loyalty and, ultimately, your bottom line. Microsoft continues to collaborate with technology vendors such as Intel to embed their latest innovations in the fabric of Azure IaaS. As a result, Azure can deliver, among other benefits, the continuous infrastructure efficiency improvements that customers expect from the cloud. Azure provides broad support for a variety of workloads on Azure IaaS, ranging from Red Hat OpenShift to SQL, Oracle® and SAP, as well as other systems. This paper focuses on our learnings of moving SAP to Azure as a key business-critical workload.

By deploying the latest Azure VMs, you can improve the performance of your applications while controlling costs.

The latest Intel-based Azure Virtual Machines feature:

- New AVX-512 instructions and architectural features parallelise execution of encryption functions, reducing penalty of implementing pervasive data encryption**, thereby generating higher throughput for encryption-intensive workloads such as SSL web server.
- Bitnami in collaboration with Intel has published two images in Azure Marketplace tailored to 3rd Gen Intel® Xeon® Scalable processors based on Azure Dv5 VMs containing Intel cryptographic software libraries.

NGNIX: https://azuremarketplace.microsoft.com/marketplace/apps/bitnami.nginx-intel

WordPress: https://azuremarketplace.microsoft.com/marketplace/apps/bitnami.wordpress-intel

With the built-in crypto acceleration provided by 3rd Gen Intel® Scalable processors, the Dv5-series VMs delivered a throughput performance increase of 58% and a reduced average wait time of 55% compared to the prior generation of Intel-based VMs. In addition, D4dsv5 executed 55% more threads than D4dsv4.

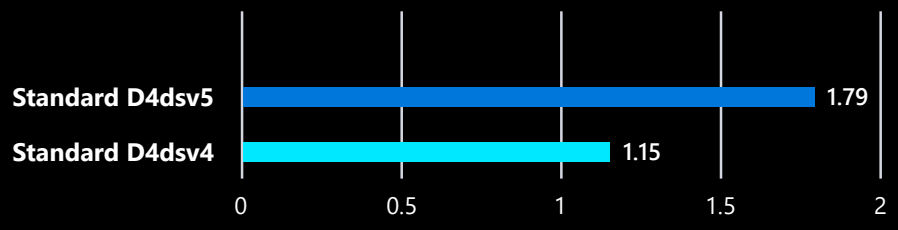


Figure 3. *Total thread execution (# in millions) – Total number of https requests executed in a 30-minute stress test*

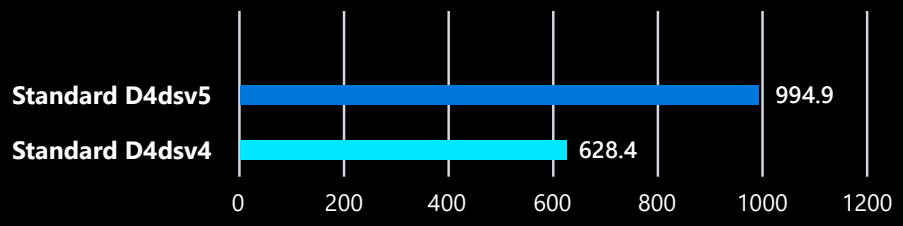


Figure 4. *Throughput (#/s) – Total number of https transactions per second*

According to a recent benchmark report prepared by Principled Technologies, the new Eds v5 VMs processed the SQL Server workload significantly faster than the previous generation VMs. The time to complete the workload can be up to 1.27x as fast for businesses using mid-sized VMs. This can benefit customers in finding data insights in less time, which can improve their business sooner.

- 1.23x for businesses using small 8 vCPUs VMs running a 30GB database
- 1.27x for businesses using mid-sized VMs with 16 vCPUs and a 100GB database
- 1.23x for businesses using large VMs with 64 vCPUs and a 300GB database

For workloads and configurations see: Principled Technology Ice Lake SQL Server Azure

MySQL database analytics perform 64% faster with 3rd Gen Intel® Xeon® Scalable processors versus prior 4th Gen.

See 81 at www.intel.com/3gen-xeon-config. Results may vary.

Database performance: Business criticality takes on additional importance when considering data input, output and transaction rates. An example is online transaction processing applications requiring high transaction rates and low IO latency. This type of system demands not only the highest resilience to failures but also fast failovers using multiple synchronously updated replicas. Azure SQL Database has a specific business-critical tier that is designed for performance-sensitive workloads. Additionally, you can migrate to Azure your on-premises MySQL, PostgreSQL, MariaDB and Apache Cassandra data estate while relying on advanced security, same-zone or zone-redundant high availability and service-level agreement (SLA) guarantees.

Reliability

Azure infrastructure is composed of geographies, regions and availability zones, which limit the blast radius of a failure, therefore limiting the potential impact to customer applications and data. The Azure availability zones construct was developed to provide a software and networking solution to protect against data centre failures and to deliver increased high availability (HA) to our customers. HA architecture creates a balance between high resilience, low latency and cost.

Assess your security requirements including the need to encrypt data while in use. With Azure confidential computing, you can choose from a broad range of hardware and software options to strengthen the security of your applications.

For example, use Azure VMs based on Intel® Software Guard Extensions for confidentiality and customisation down to the application level. Utilise Azure services such as our trusted launch feature to measure the integrity of the confidential VM. Add Azure Attestation, a unified solution that verifies the security postures of virtual machines.

Security

As previously discussed, security is paramount for most applications and systems, and even more so for business-critical systems that often are customer-facing. For cloud services such as Azure and Microsoft 365, security is supported with platform-wide Zero Trust capabilities. Microsoft and its partners can assess your Zero Trust maturity and monitor, test and improve your security and identity posture to help ensure security policies are enforced in real time.

Cost optimisation and operational agility

Your business-critical cloud journey may require you to consider tradeoffs. On the one hand, you want a resilient and scalable solution that is highly secure and conforms to applicable governance, risk and compliance requirements. On the other hand, you need to adhere to your organisation's business and IT budget guidelines. It is important to manage these tradeoffs within your specific cloud-strategy parameters. Nonetheless, moving your business-critical infrastructure to the cloud can increase operational agility, especially in a climate of business uncertainty or subject to rapid fluctuations.

05

Transitioning to the cloud: Best practices, patterns

Plan, implement and operate

Cloud migration and modernisation are continuous operations that require significant organisational change management, spanning across people, processes and technology. Taking a holistic approach not only helps you navigate the journey successfully but also helps ensure that your organisation realizes new benefits – including efficiency, agility and scale – once your workloads are running in the cloud.

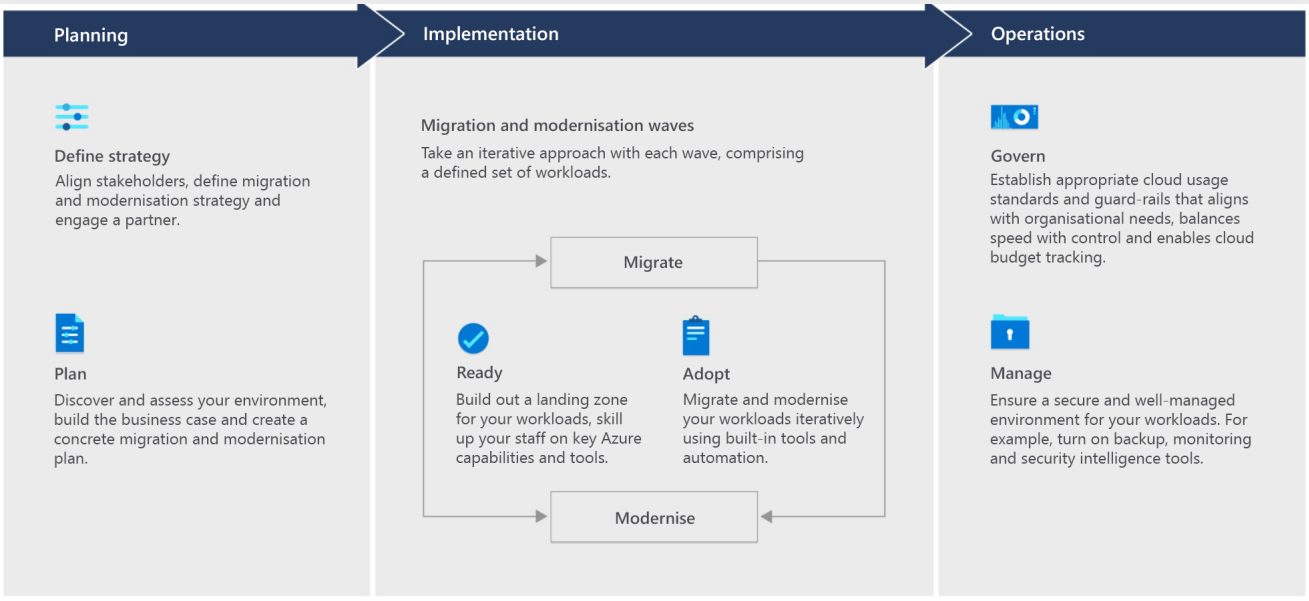


Figure 5. *Cloud Adoption Framework overview*

Transitioning business-critical workloads to the cloud requires a systematic process and phased approach. Use the three-step approach from the Cloud Adoption Framework migration methodology, which includes Assess, Deploy and Release phases for the migration of your business-critical workloads. Augment this process with the checklists for business-critical workloads.

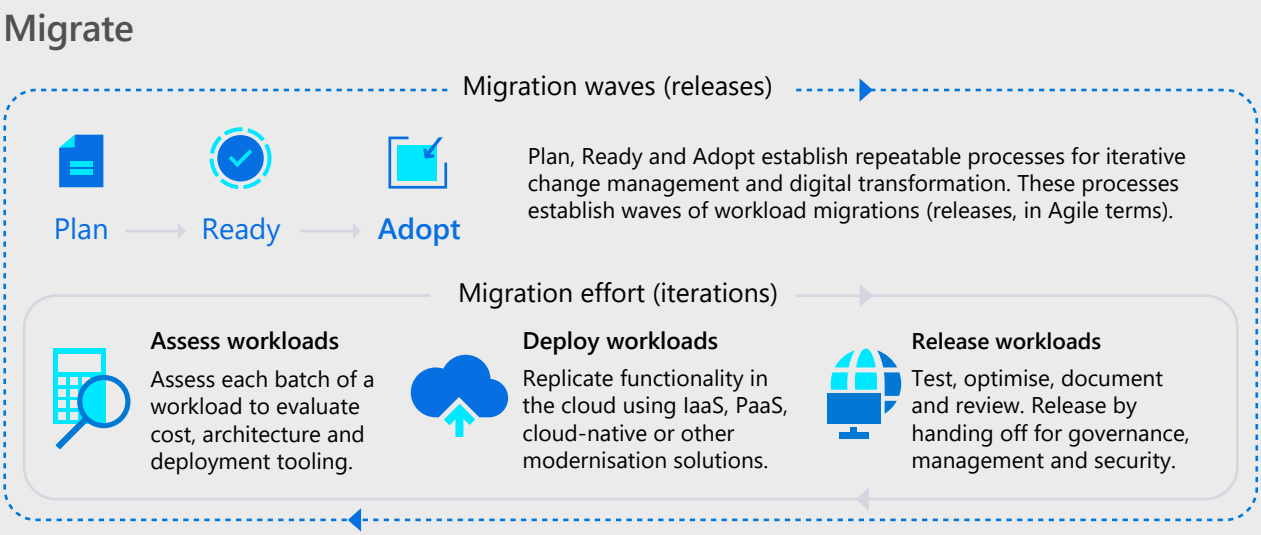


Figure 6. *Migration effort: Assess, Deploy and Release phases*

Assess workloads

While you may use Azure Migrate or ISV (independent software vendor) tools to gather information about the source environment, it is critical to involve the application architects, the subject matter experts and potentially the application vendor early in the migration process.

Use the interview process, workshops or whiteboarding sessions to understand the application architecture, business criticality and application complexity.

Deploy workloads

In this phase of the journey, you use the output of the assessment phase to initiate the migration of the environment. This guide helps identify the appropriate tools to reach a completed state. You will explore native tools, third-party tools and project management tools.

Checklist for assessing workloads

Planning

Once you've completed your assessment, it's time to prepare for the cloud migrations.

- ☐ Develop the target architecture for each environment. Perform sizing for each environment using Azure Migrate or similar tools.
- ☐ Develop approximate cost and resourcing:
  - Determine the cost of running the workload or application on Azure services.
  - Identify resource (people) requirements for the migration.
- ☐ Identify available downtime windows.
- ☐ Select appropriate Azure subscriptions and regions for solution or workload deployment.
- ☐ Settle on a cloud deployment strategy:
  - Identify the system components that must be deployed on Azure IaaS Virtual Machines.
  - Determine the system components and interfaces that will continue to stay on-premises.
  - Identify the application components that could be modernised and deployed on Azure PaaS, such as using Azure SQL Database, Azure App Service, et cetera.
  - Finalise compute, storage, networking and database selections in support of your business-critical workloads.
- ☐ Determine the appropriate encryption and security hardening strategy. In addition, create identity and security controls.

Intel® Software Guard Extensions (Intel® SGX) technology allows customers to create enclaves that protect data, keeping data encrypted while the CPU processes it. The operating system (OS) and hypervisor can't access the data. Data centre administrators with physical access also can't access the data.

Enclaves are secured portions of the hardware's processor and memory. You can't view data or code inside the enclave, even with a debugger. If untrusted code tries to change content in enclave memory, Intel® SGX disables the environment and denies the operations. These unique capabilities help you protect your secrets from being accessible in the clear.

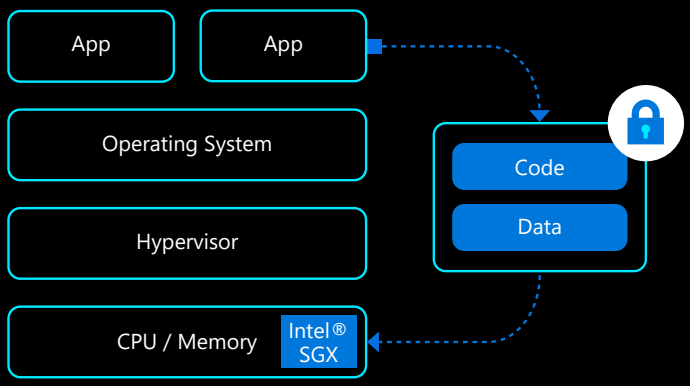


***Figure 7**. Enclave pathways overview*

Think of an enclave as a secured lockbox. You put encrypted code and data inside the lockbox. From the outside, you can't see anything. You give the enclave a key to decrypt the data. The enclave processes and re-encrypts the data, before sending the data back out.

Each enclave has an encrypted page cache (EPC) with a set size. The EPC determines the amount of memory that an enclave can hold. DCsv2-series VMs hold up to 168 MiB. DCsv3/DCdsv3-series VMs hold up to 256 GB for more memory-intensive workloads.

- ☐ Analyse the impact of network latency on application performance.
- ☐ Understand communication with different interfaces and ports using tools like Azure Migrate dependency analysis, Service Map or Cloudscape.
- ☐ Use Service Map to collect the volume of data and latency between different interfaces. Assess the impact of latency, and identify the bandwidth requirement.
- ☐ Develop test plans if they do not already exist.
- ☐ Identify opportunities to automate and standardise the deployment process using tools such as Azure DevOps Pipelines, Infrastructure as Code (IaC) templates, Jenkins, Ansible, et cetera.
- ☐ Plan for monitoring, patching and upgrades as well as backup solutions.
- ☐ Create a high-availability and disaster-recovery approach.
- ☐ Plan for technical training for the support and operations team. In addition, arrange process training if there are changes to operational processes.
- ☐ Be aware of key anti-patterns:
    - Avoid making any functional enhancements to the application during the migration process.
    - Avoid making major architectural changes to the application during the migration process.

Deployment using Infrastructure as Code

Infrastructure as Code is a set of techniques and practices that helps IT pros remove the burden associated with the day-to-day build and management of modular infrastructure. It allows IT pros to build and maintain their modern server environment in a way that is similar to how software developers build and maintain application code.

- ☐ Deploy the workload as per reviewed and approved target architecture.
- ☐ Use Infrastructure as Code templates and automation to build the environment.
- ☐ Perform any post-deployment configurations.
- ☐ Perform any post-migration security hardening.

Key learnings from recent customer migrations

- Automate, automate, automate. Treat everything as code; software that is not automatable is broken.
- Stay motivated. Build and deploy your infrastructure, workloads and applications more often.
- Anything and everything that is required to be built and deployed must exist in source control.
- Make a habit of pushing into production regularly.
- Avoid repeating manual fixes. Every time you've done something for the third time, automate it.
- No test should remain un-automated that could be automated. This includes unit, smoke, functional and end-to-end testing.
- Establish consistency in communications with regular scrum calls.
- Remember, the production environment should be reproduced on demand if required.
- Focus on adoption and change management to deal with culture changes in migrating workloads to the cloud.

Release workloads

This phase is also an opportunity to optimise your environment and perform possible transformations of the environment. For example, you may have performed a "rehost" migration, and now that your services are running on Azure, you can revisit the solutions configuration or consumed services and possibly perform some "refactoring" to modernise and increase the functionality of your solution.

Checklist for releasing workloads

- ☐ Leverage your test plans to execute performance testing and document the results. Compare the performance of your system with an on-premises performance baseline. Identify any performance bottlenecks and make appropriate changes, for example by scaling Azure resources or by adding caching for faster data retrieval.
- ☐ Conduct user acceptance testing and perform testing for high availability and disaster recovery.
- ☐ Use appropriate bug tracking systems such as Azure DevOps or Jira to raise, track and resolve any bugs. Document and resolve any reported issues.
- ☐ Review workload configurations for data compliance and data security.
- ☐ Add potential enhancements or updates to your DevOps backlog.
- ☐ Execute your cutover plan:
  1. Perform data synchronisation and data refresh.
  2. Make appropriate change to DNS.
  3. Redirect partial user traffic to resources on Azure.
  4. Monitor the performance matrices.
  5. Repeat steps 3 and 4 to redirect additional user traffic to Azure.
  6. Perform the final cutover as appropriate.
- ☐ Decommission your source servers.
- ☐ Optimise workloads over time to gain additional operational agility:
  - Consider using cloud-native technologies for monitoring and management of your applications.
  - Consider modernising your applications components to run on PaaS or SaaS.
  - Use pay-as-you-go capabilities to your advantage. Scale down your environment when not needed.
  - Use cloud-native cost optimisation tools to help lower the cost of running your workloads.

Business-critical checklists

The following checklists provide Azure cloud migration best practices that go beyond the basic cloud-native tools. These checklists outline the common areas of complexity that often occur in business-critical workloads and that might require the scope of the migration to expand beyond the Azure migration guide.

- ☐ VMware migration: Migrating VMware hosts can accelerate the overall migration process. Each migrated VMware host can move multiple workloads to the cloud. After migration, those VMs and workloads can stay in VMware or be migrated to modern cloud capabilities.
- ☐ SQL Server migration: Migrating instances of SQL Server can accelerate the overall migration process. Each migrated instance can move multiple databases and services, potentially accelerating multiple workloads.
- ☐ Multiple data centres: Migrating multiple datacenters adds significant complexity. During each process of the move (assess, migrate, optimise and manage), other considerations are discussed to prepare for more complex environments.
- ☐ Data requirements exceed network capacity: Companies frequently choose to migrate to the cloud because the capacity, speed or stability of an existing data centre is no longer satisfactory. However, those same constraints add complexity to the migration process, requiring additional planning during the assessment and migration processes.
- ☐ Governance or compliance strategy: When governance and compliance are vital to the success of a migration, IT governance teams and the cloud adoption team must ensure additional alignment with one another.

Operations and security

Operational excellence covers the operations and processes that keep an application running in production. Deployments must be reliable and predictable, automated to reduce the chance of human error while ensuring fast and routine processes to release new features and bug fixes. The ability to quickly roll back or roll forward if an update has problems is equally important.

These are the core pillars to consider before starting the journey of operations:

- Encryption at rest, in transit and while data is in use
- Hardening
- Network isolation and controls
- Patching – Azure Update Management
- External publishing
- Vulnerability management
- Threat detection and protection
- Anti-malware
- Management groups hierarchy
- Audit and logging
- Azure policy
- Alerts and notifications

Figure 8. *Core operations pillars checklist*

Regarding security, follow the defense in depth approach to secure all your workloads.

Defense in Depth

Identity & access	Apps & data security	Network security	Threat protection	Security management
Role based access	Encryption	DDoS Protection	Antimalware	Log Management
Multi-Factor Authentication	Confidential Computing	NG Firewall	AI Based Detection and Response	Security Posture Assessment
Central Identity Management	Key Management	Web App Firewall	Cloud Workload Protection	Policy and governance
Identity Protection	Certificate Management	Private Connections	SQL Threat Protection	Regulatory Compliance
Privileged Identity Management	Information Protection	Network Segmentation	IoT Security	SIEM

Microsoft + Partners

Figure 9. *Defense in depth approach*

Deep dive for business-critical workloads: Migrating SAP to Azure IaaS

Let's explore business-critical migration practices by delving deeper into an example of SAP-to-Azure migration. For many companies, SAP is used to run key business processes like enterprise resource planning, customer relationship management and supply chain management. In some cases, the SAP estate is large, with complex interdependencies. As such, it is worth examining as a business-critical system that requires special consideration when migrating to the cloud. SAP is the perfect candidate for the Azure Cloud Adoption Framework since it's often the "circulatory and nervous system" equivalent of a business.

Discovery

Ensure that you fully understand the design and "sizing" of the current on-premises SAP systems so that you can accurately size and design the target environment.

Discovering small but critically dependent components of old legacy systems that are lost in the configuration databases, or lost due to changes in staffing, is a common challenge.

Custom "sourced code" systems and appliances can also create challenges as the OEM vendor may not be in business anymore, or the support is dropped for a newer package, which may require a major overhaul when migrating. Pay special attention to legacy applications running on non-x86/x64 platforms and custom-code solutions.

Learn more about SAP workloads on Azure with the planning and deployment checklist ›

Target environment

Ensure that the target Azure environment has been deployed and thoroughly tested before you commit to migrating and moving SAP systems. Following the Cloud Adoption Framework SAP-specific guidance can help with your journey to the cloud.

Learn more about enterprise-scale for SAP on Azure ›

VM sizing

Deploying IaaS VMs creates equal or greater performance than on-premises, although the virtual machine and disk SKUs can be scaled up or down as requirements change.

- Use the SAP values, provided to ensure that the VM choice is performing well enough.
- Ensure that the VM is certified by SAP (not all VMs are certified, but non-certified can be used in non-production environments).
- Make sure that you use SAP-certified OS images.
- Design every SAP system with the network and storage latency in mind.

For VMs hosting, HANA databases, or an equivalent in-memory database engine, a general rule is to select a VM size that supports a memory capacity of at least 1.2x the database size. In general, you can use the virtual machine selector to help expedite the VM and disk storage selection process.

Learn more about sizes for virtual machines in Azure ›

SAP on Azure solutions help you optimise your enterprise resource planning (ERP) in the cloud using the security features, reliability and scalable SAP-certified infrastructure of Azure.

You can choose to deploy SAP-certified on-demand virtual machines for SAP NetWeaver applications such as SAP Business Suite, as well as SAP HANA-based applications such as SAP S/4HANA.

You can also choose purpose-built SAP HANA infrastructure (SAP HANA Large Instances), which offers high-performance compute, storage and network. The HANA Large Instances are powered by Intel® Xeon® Scalable processors and feature Intel® Optane™ persistent memory (Intel® Optane™ PMem), offering higher performance and lower TCO benefits.

- SAP HANA-certified IaaS instances with memory from 768 GB to 24 TB and 2 socket to 16 socket supporting up to 896 vCPUs.
- Certification for SAP S/4HANA, SAP BW/4HANA, SAP BW on SAP HANA and Suite on SAP HANA.
- Industry-leading performance with high-performance NFS storage and networking.
- High availability, disaster recovery, scale-out configurations and built-in support for backups.
- Snapshot-based backups of 24TB database in minutes.
- Only public cloud that offers Intel® Optane™ PMem to deliver faster time to insights, simplified IT infrastructure and lower costs.

Disks

Ensure that the disks attached to the VM are functional (IOPS, throughput, etc.) for the specific application.

Learn more about Azure-managed disk types ›

The following table provides a comparison of the four disk types to help you decide which to use.

	Ultra disk	Premium SSD	Standard SSD	Standard HDD
Disk type	SSD	SSD	SSD	HDD
Scenario	IO-intensive workloads such as SAP HANA, top tier databases (for example, SQL, Oracle) and other transaction-heavy workloads	Production and performance sensitive workloads	Web servers, lightly used enterprise applications and dev/test	Backup, non-critical, infrequent access
Max disk size	65,536 gibibyte (GiB)	32,767 GiB	32,767 GiB	32,767 GiB
Max throughput	4,000 MB/s	900 MB/s	750 MB/s	500 MB/s
Max IOPS	160,000	20,000	6,000	2,000

Figure 10. *Virtual machine disk-type comparison*

Production SAP systems should follow the recommended storage configuration guidelines below, but the "cost-conscious" option can be used for non-production systems.

Ensure that the chosen VM and disk storage combinations are well suited to handle the VM-to-disk-storage throughput the application demands. This is particularly important with online transaction processing (OLTP) scenarios.

Learn more about SAP HANA Azure virtual machine storage configurations ›

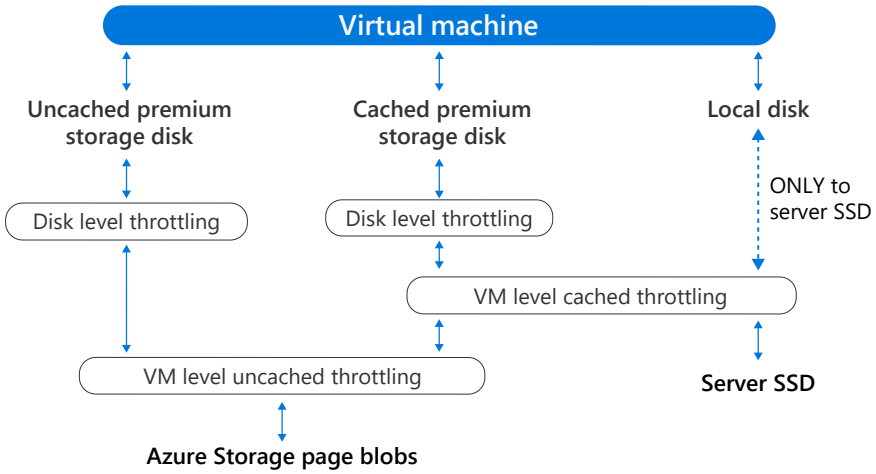


Figure 11. I/O throttling concept

Learn more about virtual machine and disk performance ›

Azure NetApp Files (ANF)

Consider use of ANF to complement the Azure disk options where increased performance and/or very low recovery time objective (RTO) or very low recovery point objective (RPO) are required. ANF can offer performances up to 512 Mbps per 4 TB pool of Ultra tier.

Learn more about Azure NetApp Files ›

A key advantage of using ANF is the capability to instantly take a volume snapshot without disrupting existing disk operations. This makes performing backup and restore of massively sized databases very quick. Azure now offers an application-consistent snapshot tool that can ease the process of snapshot backup, restore and volume clone.

Learn more about the Azure Application Consistent Snapshot tool ›

Reinvest capital from reduced TCO gained through simplified IT infrastructure and higher memory densities.

Reduce operational and licensing costs through node consolidation with (Intel® Optane™ PMem) configurations.

You can run SAP installations in non-business-critical environments on same hardware with separate storage allocations:

- Best-fit solution for your needs and budget with the broadest portfolio of certified SAP options
- Lower TCO than typical on-prem solutions – and pay for only what you use
- More memory at the same cost with a scale-up SAP HLI solution
- Outstanding performance-per-dollar when you choose Intel® technology for your cloud workloads

See also: "Next Generation SAP HANA Large Instances with Intel® Optane™ drive lower TCO." April 2020. https://azure.microsoft.com/blog/next-generation-sap-hana-large-instances-with-intel-optane-drive-lower-tco/

Cost

Once you've sized the required VMs and associated resources, it's important to calculate the total cost of what you plan on deploying since it may be more than anticipated. "Reserved instances" and the use of "cost-conscious" options can help reduce the total monthly spend.

Use the Azure Pricing Calculator to correctly determine pricing for your SAP VMs. OS licensing is a significant component of SAP infrastructure. Use pay-as-you-go pricing instead of bring-your-own licensing (BYOL) for Red Hat Enterprise Linux and SUSE Linux Enterprise.

Learn more about cost with the Azure Pricing Calculator ›

RTO/RPO

Fully understand and document the required RTO and RPO for the SAP systems and ensure that whichever backup solution you plan meets the requirements. The Azure native backup solution supports the backup/restore of SAP HANA databases.

For extremely small RTO/RPO, consider using Azure NetApp Files and the volume snapshot feature as backing volumes for your workloads.

Learn more about the support matrix for backup of SAP HANA databases on Azure VMs ›

Learn how the Azure NetApp Files snapshots work ›

High availability

Consider the use of multiple server instances and clusters to provide high availability, along with availability zones that can help provide protection against the loss of data centres in a particular region. This is particularly important for HANA database instances.

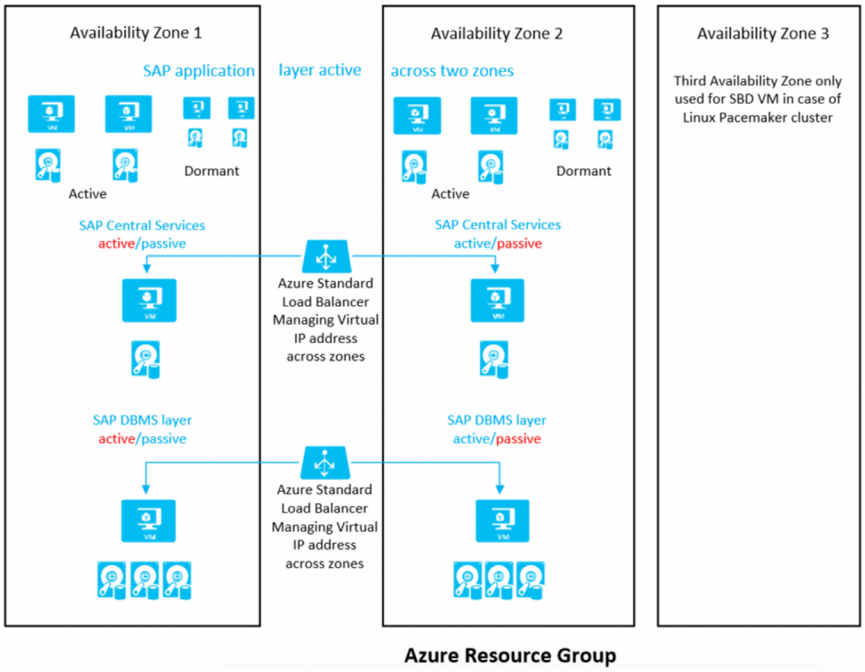


Figure 12. *SAP configuration using Azure availability zones*

Learn more about SAP workload configurations with Azure availability zones ›

Disaster recovery

It is essential to plan, design and fully test disaster recovery before migrating any production SAP systems. This helps ensure that the key systems keep running and that they can quickly be brought back online in another region. Disaster-recovery sites must be tested regularly with a test failover activity to ensure DR health.

When using ANF, SnapMirror volume can be used to replicate your volumes to another NetApp volume in a paired region. The replication can be configured in as little as 10 minutes with an RPO of 20 minutes for landscapes where a SAP HANA system replication site is cost-prohibitive.

Learn more about the cross-region replication of Azure NetApp File volumes ›

Testing

Once the new SAP systems have been deployed and configured, it is crucial to carry out as much testing as possible before you migrate. This needs to include functional testing as well as performance testing and requires input from the SAP Basis team and the product owners/stakeholders.

Security

Infrastructure security should be included as part of the landing zone design/deployment. It uses a combination of role-based access control (RBAC) roles and policy to enforce the required guidelines and access. The SAP layer of security can then be added or migrated over the top of this as part of the migration process.

Learn more about security in the Microsoft Cloud Adoption Framework for Azure ›

Business alignment

Risk insights
Integrate security insights into risk management framework and digital initiatives.

Security integration
Integrate security insights and practices into business and IT processes; integrate security disciplines together.

Business resilience
Ensure organisation can operate during attacks and rapidly regain full operational status.

Security disciplines

Access control
Establish Zero Trust access model to modern and legacy assets using identity and network controls.

Security operations
Detect, respond and recover from attacks; hunt for hidden threats; share threat intelligence broadly.

Asset protection
Protect sensitive data and systems. Continuously discover, classify and secure assets.

Security governance
Continuously identify, measure and manage security posture to reduce risk and maintain compliance.

Innovation security
Integrate security into DevSecOps processes. Align security, development and operations practices.

Figure 13. *SAP and Cloud Adoption Framework secure methodology*

Governance

Similar to security, governance should be included as part of the infrastructure design/deployment using management groups, policy and RBAC.

Learn more about governance in the Microsoft Cloud Adoption Framework for Azure ›

Govern

Define corporate policy

Business risks

Document evolving business risks and the organisation's tolerance for risk, based on data classification and application criticality.

Policy & compliance

Convert risk decisions into policy statements to establish cloud adoption boundaries.

Process

Establish processes to monitor violations and adherence to corporate policies.

Five disciplines of cloud governance

Cost management

Evaluate and monitor costs, limit IT spend, scale to meet need, create cost account-ability.

Security baseline

Ensure compliance with IT security requirements by applying a security baseline to all adoption efforts.

Resource consistency

Ensure consistency in resource configuration. Enforce practices for onboarding, recovery and discoverability.

Identity baseline

Ensure the baseline for identity and access is enforced by consistently applying role definitions and assignments.

Deployment acceleration

Accelerate deployment through centralisation, consistency and standardisation across deployment templates.

Figure 14. *Cloud Adoption Framework governance model*

Deployment

Avoid manual deployment whenever possible. Take advantage of the SAP HANA deployment toolchain to automate deployment of your SAP infrastructure and utilise the included Ansible playbooks to deploy the SAP Basis foundation. Combine these with the Azure Cloud Adoption Framework Terraform toolchain to automate and ease the deployment of the most complex environments.

To simplify production to non-production refresh activities, encourage the adoption of the DevOps and site reliability engineering approach. Build pipelines in Azure DevOps to automate regularly occurring tasks such as non-production deployment and building tests.

Monitoring

Consider using the SAP-specific monitoring solution (currently in preview) to monitor the various logs and metrics from the new infrastructure. Ensure that you have the virtual machines and associated resources configured to send all details to a Log Analytics workspace.

Learn more about monitoring SAP on Azure ›

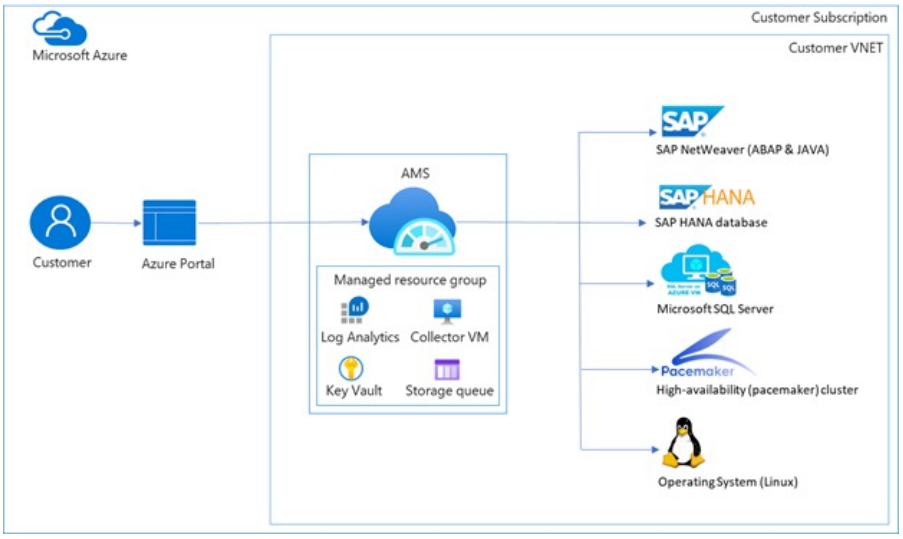


Figure 15. Azure Monitor for SAP solutions architecture

06

Business-critical partner ecosystem

Many organisations we work with are eager to realise myriad benefits for their own business-critical applications, but first they need to address questions about their cloud journey, including:

- **Are the core applications I use on-premises certified and supported on Azure?**
- **As I move to Azure, can I retain the same level of application customisation that I have built over the years on-premises?**
- **Will my users experience any impact in the performance of my applications?**

In essence, you want to make sure you can continue to capitalise on the strategic collaboration you've forged with your partners and ISVs as you transition your core business processes to the cloud. You want to continue to use the very same applications that you spent years customising and optimising on-premises.

Microsoft understands that running your business on Azure goes beyond the services and capabilities that any platform can provide. You need a comprehensive ecosystem. Azure has always been partner-oriented, and we continue to strengthen our collaborations with a large number of ISVs and technology partners so you can run the applications that are critical to the success of your business operations on Azure.

We work with many partners to create effective and efficient migration strategies, plans and services for highly complex and business-critical workloads. Our in-house teams can support all stages of your business-critical migration journey. We're expanding the many ways we can further deliver value to your organisation.

While we partner with ISVs and global and regional systems integrators, we also work more specifically with tool vendors to support automated discovery, workload analysis and more. Because Azure supports many open-source systems, we're able to leverage partnerships that specialise in those types of solutions.

Read our blog post that provides an in-depth overview of our business-critical partnerships ›

07

Next steps

We hope with this eBook you feel better prepared to modernise your business-critical systems and applications with the cloud. We've identified business-critical apps and systems and explained the risks and benefits of moving them to the cloud, based on suggested migration and modernisation approaches. Please explore the next steps below and resources in the appendix to learn how Microsoft can assist with your cloud transformation journey.

Are you considering migration for your business-critical workloads?

Contact a Microsoft partner to learn about the Azure cloud services and programmes that can help support your cloud transformation journey. Learn how partnering with Microsoft can help you develop a secure and reliable migration strategy for your business-critical workloads.

Get started with Cloud Adoption Framework for Azure ›

Are you exploring your first business-critical workload migration?

If you are exploring migration of business-critical workloads to Azure, a Microsoft partner can help you plan and build an Azure enterprise-scale landing zone to pilot your initial business-critical workload. You can also continue to build Azure developer and operational skills by learning about the Azure cloud services and programmes than can support a reliable and secure cloud transformation journey.

Learn about the Azure Migration & Modernization Program ›

Are you ready to move business-critical workloads to Azure?

If you're ready to start your migration of business-critical workloads at scale, schedule a cloud transformation envisioning workshop with a Microsoft partner today. We can help build and execute a roadmap of your migration engagement and provide support for your cloud transformation journey.

Get started with Azure cloud transformation ›
(English only)

08

Appendix: Resources

These resources provide our customers with the necessary tools and information to effectively manage and migrate their workloads to Azure.

Well-Architected Framework

The Azure Well-Architected Framework (WAF) is a set of guiding tenets that can be used to improve the quality of a workload. The framework consists of five pillars of architectural excellence: cost optimisation, operational excellence, performance efficiency, reliability and security. Incorporating these pillars helps produce high-quality, stable and efficient cloud architectures.

WAF Pillar	Description
Cost Optimisation	Managing costs to maximise the value delivered.
Operational Excellence	Operations processes that keep a system running in production.
Performance Efficiency	The ability of a system to adapt to changes in load.
Reliability	The ability of a system to recover from failures and continue to function.
Security	Protecting applications and data from threats.

Figure 16. *Well-Architected Framework pillars*

Learn more about Microsoft Azure Well-Architected Framework ›

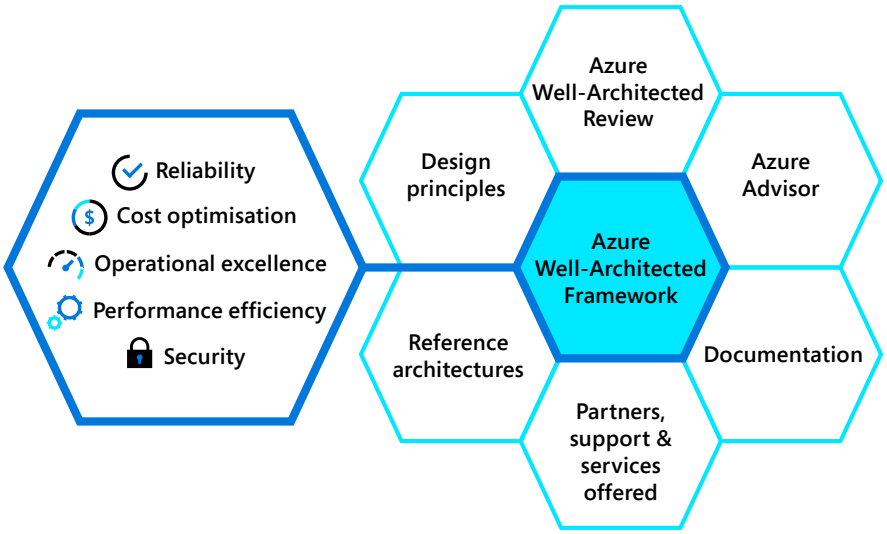


Figure 17. *Azure Well-Architected Framework*

Cloud Adoption Framework

The Cloud Adoption Framework for Azure is a collection of documentation, technical guidance, best practices and tools that aid in aligning business, organisational readiness and technology strategies. This alignment enables a clear and actionable journey to the cloud that rapidly delivers on the desired business outcomes.

The Cloud Adoption Framework helps customers undertake a simplified cloud journey in four main stages:

1. Define strategy
2. Plan
3. Ready
4. Adopt

Learn more about the Cloud Adoption Framework ›

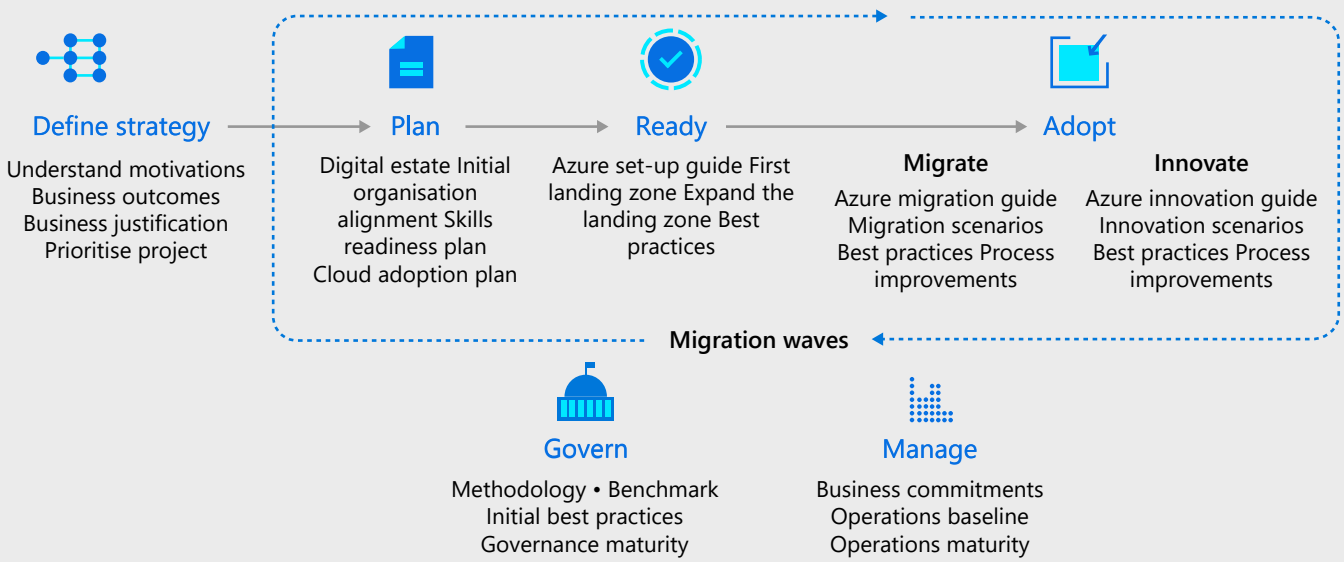


Figure 18. *Cloud Adoption Framework overview*

Azure Architecture Centre

The Azure Architecture Centre is a useful resource for browsing all the architecture patterns and finding best practices for building applications on Microsoft Azure.

Learn more about technology areas with the Azure Architecture Centre ›

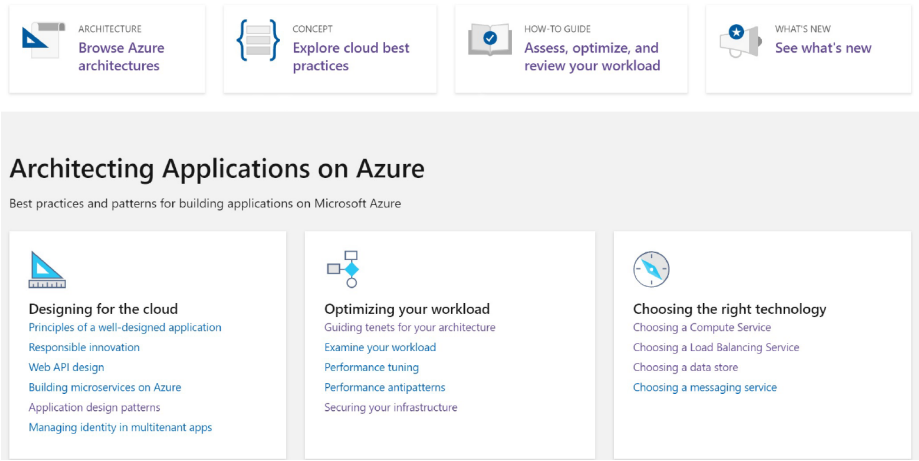


Figure 19. *Azure Architecture Centre*

SAP on Azure Architecture Guide

The SAP on Azure Architecture Guide describes a set of guiding tenets used to help ensure the quality of SAP workloads running on Azure. This guide is based on the Microsoft Azure Well-Architected Framework, but the recommendations are specific to deployments of SAP solutions. A solid architectural foundation starts with the five pillars of excellence: cost, DevOps, resiliency, scalability and security.

- Overview
- SAP HANA on Azure (Large Instances)
- SAP HANA scale-up on Linux
- SAP NetWeaver in Windows on Azure
- SAP S/4HANA in Linux on Azure
- SAP BW/4HANA with Linux VMs on Azure
- SAP NetWeaver on SQL Server
- SAP deployment on Azure using an Oracle DB
- Dev/test for SAP workloads on Azure

Cloud assessment and risk assessment

Customers can evaluate their business strategies and receive curated guidance from Microsoft Assessments.

- Azure Well-Architected Review
- Cloud Journey Tracker
- Developer Velocity
- Governance Benchmark
- Strategic Migration Assessment and Readiness Tool

Learn about the available assessments ›

Learn more about risk assessment with the guide for Microsoft cloud compliance ›

Public case studies

- USA | Albertsons | Retail | Microsoft Customer Story – Albertsons and Microsoft partner on cloud adoption to enable digital transformation
- UK | Bristol City Council | Public Sector | Microsoft Customer Story – Bristol City Council unlocks its ability to innovate and sets the stage for true digital transformation
- Mexico | SAE | Microsoft Customer Story – SAE Digital Transformation Initiative
- UK | Benenden School | K–12 | Microsoft Customer Story – Benenden School adopts hyperconverged infrastructure and remote learning with Azure Stack HCI and Intel
- USA | MobileCoin | Banking and Capital Markets | Microsoft Customer Story – MobileCoin creates fast, trusted cryptocurrency transfers with Azure confidential computing
- UK | Buro Happold | Professional Services | Microsoft Customer Story – Buro Happold creates sustainable, striking environments with Azure high-performance computing fueled by Intel
- Canada | Royal Bank of Canada | Banking and Capital Markets | Microsoft Customer Story – RBC creates relevant personalised offers while protecting data privacy with Azure confidential computing
- SAP on Azure solutions customer stories
- Business-critical applications on Azure customer stories

Programmes and offerings

- AMMP: Azure Migration and Modernization Program
- Cloud Transition Services: Accelerating modernisation and enabling innovation on the Microsoft cloud (English only)