AZURE RAPID, LARGE-SCALE MIGRATIONS

8 Strategies Critical for a Successful Cloud Migration
1.0 Seven Strategies Critical for a Successful Cloud Migration

1.1 Large-Scale, Rapid, and Secure Azure Cloud Migration

1.2 Discovery, Validation, Assessment, and Planning

1.3 Automated Rapid Migration

1.4 Azure Cloud Migration with DevSecOps

1.5 Azure Hybrid Cloud-Enabled Networking

1.6 Security Approval Acceleration and Secure Legacy Workloads

1.6.1 Templated Security Control Automation and Secure Configuration Compliance Automation

1.6.2 Secure Hybrid Workloads with Greater Security Requirements

1.7 Azure Cloud Management

1.8 Migration Factory Project Approach Using Azure Migration Service

2.0 SUMMARY
1.0 Seven Strategies Critical for a Successful Cloud Migration

The trend is clear: If you aren’t in the cloud, you are falling behind. But for you to realize true cloud success, you should consider carefully how you will strategically and tactically deploy the cloud to benefit your organization. It’s no surprise that many IT executives see some significant disadvantages when first deploying the cloud, including:

- Higher costs than expected
- Longer time frame for migration
- Lack of internal expertise to fully exploit cloud
- Difficulty managing hybrid and multicloud

Therefore, for your organization to achieve genuinely useful digital transformation, it’s important that you take advantage of the operational and cost benefits of Azure-based cloud deployments with careful planning, especially in large-scale deployments. Otherwise, you may see only marginal (and disappointing) returns on your investment. Also, integrating emerging technologies can be risky and challenging. You may have thousands of legacy applications that need to be modernized and migrated in some fashion. Your ability to control costs and speed Azure adoption are crucial factors, requiring large-scale automation and assured security, along with an imperative to keep your operations up and running during the transition.

New applications can be developed in a cloud environment using modern cloud technology and a DevSecOps methodology. By using DevSecOps to automate software deployment, you can ensure consistent and repeatable deployments that limit the risks of introducing security vulnerabilities. You also can safely roll back deployments at any time.

Seven Strategies for Azure Migrations

For existing applications and workloads hosted in data centers, you have a number of options to consider in migrating to Azure public clouds or Azure Stack private clouds, including “Lift and Shift” and container migration, which can reduce complexity while improving portability and scalability.

Devising a migration plan for each application system, prioritizing actions, developing the proper migration sequence, and meeting associated security and performance requirements are critical elements for your cloud migration projects. Mission requirements, business priorities, operational challenges, budget constraints, regulatory mandates, and other issues must drive the decision on migration strategy for each application or group of applications.

The bottom line? Implementing a bulk migration to the Azure cloud requires the right partners, skills, and solutions to avoid delays and unforeseen problems.
While each cloud migration project is unique, all successful large-scale enterprise workload migrations to Azure share some core building blocks, including:

- Ensure success with thorough, automated discovery, assessment, and planning
- Use a repeatable “Azure migration factory” methodology that includes introduction of enterprise shared-service standards
- Perform agile-based planning/replanning migration management
- Utilize continuous integration/continuous delivery (CI/CD) for DevOps/DevSecOps-enabled customers
- Deploy a migration management portal to track overall progress
- Use an end-to-end cloud migration life cycle that ensures that optimal performance is maintained at the enterprise and application levels
- Deploy comprehensive security and compliance

If your organization has thousands of applications in its service portfolio, recoding all applications for migration likely will be very time-consuming and costly. In the meantime, you still need to continue operating your data center, manage your infrastructure assets, and deal with all the capital expenditure required for refresh and capacity expansion. These challenges are more than simple annoyances. Every day that passes while locked in the data center translates into:

- **Cost inefficiency.** Costs associated with facilities, labor resources, hosting operation, assets, and hard-to-automate or -integrate operations in managing your existing data centers are unavoidable.
- **Risk with instability.** Often what drives cloud migration is an unstable facility, inadequate capacity, or lack of skilled resources in the current data centers.
- **Inability to execute.** Your organization is unable to execute against a challenging environment depending on the challenges in the current business cycle.
- **Unachievable speed.** You need to deliver services faster than ever before. It is an impossible task, however, when computing capacity cannot be provisioned on demand in a flexible, reliable, and elastic fashion with cost transparency.
Rapid and secure migration to Azure can result in immediate cost savings for your organization through a reduction of facilities management, physical assets, and data center operations. Savings from data center consolidation/reduction/elimination, efficiency in application hosting services, and transition from capital expense (CapEx) to operating expense (OpEx) then can be allocated to your application modernization. This reallocation of cost savings resolves the budget challenges facing most information technology (IT) organizations in IT modernization and digital transformation. The faster and more reliably that cloud migration can be performed, the higher the return on your investment.

Your Azure cloud adoption is a journey that requires Agile-based continual assessment and optimization for improving performance, service effectiveness, and cost efficiency. Use a structured approach to your migration with sprint-focused cloud migration planning/replanning and cloud services life cycle management.

Discovery, assessment, and cloud planning include detailed considerations of your business factors, people and organization, governance, applications and data assessment (including cloud suitability, interfaces, and affinity to other client applications), technical infrastructure/platform, security, and operations management.

Engagement and communication with your organization is methodically planned and executed via Organizational Change Management (OCM) methodology.

Migrating applications and workloads to Azure is just the first step of your cloud journey. To realize all the benefits, it’s important for you to implement effective governance in security, workload life cycle management, and expense optimization. In addition, it is imperative to leverage Microsoft security native services in Software-as-a-Service (SaaS) and Platform-as-a-Service (PaaS) platforms. Cloud-agnostic and Microsoft native cloud services provide cost-effective, innovative, flexible, and readily available building blocks for enabling bimodal IT and allowing your organization to deliver services with agility and efficiency.

### 1.1 Large-Scale, Rapid, and Secure Azure Cloud Migration

You face plenty of challenges in performing Azure cloud migrations, particularly if your environment has thousands of workloads or supports many organizations and customers. Planned or executed improperly, your migration can be a complex and difficult operation, leading to significant efforts, cost, and risk.

Using best practices with a set of mature processes and proven automation solutions gives you the best chance for cloud success. We can apply our processes and automation to all kinds of workloads for accelerating the “rehost,” “replatform,” and “refactoring” migration of an overabundance of workloads to Azure. Using our solutions, you can benefit from large-scale, rapid, and secure Azure migration that is easily manageable, highly automated, resource efficient, and without compromise or downtime to your business operations. You will be able to simplify and automate workload migrations, ensure highly automated configuration remediation for security compliance, and deploy flexible and effective compensating security control, all while saving substantial time and generating cost savings.

A thorough Azure migration plan By offers you effective processes and technologies to address the three major migration phases: 1 discovery, validation, assessment, and planning; 2 migration; and 3 acceleration of security approvals and security protection of legacy workloads and applications that do not initially comply with security configuration standards.

By using a cloud migration service catalog manual with tiered, fixed unit prices, you can order exactly the cloud migration services you need. Select a migration partner that offers fixed prices for different tiers of discovery and an Azure migration planning service based on the size of your source data center. Fixed per-server migration pricing should cover all three Azure tiers, based on the data size and server system complexity. Cost transparency, service flexibility, and low project risk are essential.

Should you need on-demand capacity to migrate your workload, look for a Core-Flex capacity model. This involves establishing the baseline team for migrating your workload at fixed cost based on the established KPIs (e.g. number of servers per month). This should be flexed up in response to demand.
1.2 Discovery, Validation, Assessment, and Planning

It is critical that you have a complete understanding of the inventory and interdependencies of the workloads and applications before Azure migration. You should assess the maturity level of IT service management at your organization. Do you have rigorous control and accurate knowledge of asset inventory, system/network/application/security configurations, application dependencies, interfaces, capacity, and performance? It is important for you to validate the inventory, configuration, and dependency information before beginning any migration.

To achieve a complete assessment, you will need a highly cost-effective, high-value, lightweight solution for source data center discovery. It is important that the system is aligned with or even adds to Microsoft’s best practice migration framework. With agentless discovery, a preferred solution, you will be able to perform the following discoveries:

- Simple Network Management Protocol (SNMP)
- Load balancer
- Hypervisors and virtual machines (VMs)
- Operating system (OS)
- Domain Name System (DNS) sync and ping sweep
- Intelligent Platform Management Interface (IPMI) auto-discovery
- Services auto-discovery
- Automated application mapping
- Network and firewall topology
- Azure cloud native services

You also can access Representational State Transfer (REST) Application Programming Interfaces (APIs) and out-of-the-box connectors for other configuration management database (CMDB) tools that exist in your environment. This solution lets you automatically build knowledge of your network environment, systems, and applications, as well as the interactions and dependencies among them. And you can validate data in the source data center organization’s knowledge and configuration database. In combination with application performance management tools available in your organization, such as AppDynamics, New Relic, or Dynatrace, you can use the Unisys solution to build application profiling that includes application architecture, performance metrics, transaction patterns, user journey, and associated business processes.

Using a set of checklists that include triage decision trees, you can assess the cloud readiness of each workload and application based on the data acquired from the discovery activities. The readiness assessment provides one of the following outcomes: 1 ready to move; 2 cannot be moved without significant efforts to modify the application; and 3 while not currently ready for rehost migration, the workloads can be replatformed or refactored to Azure relatively easily within a short time. You should then plan the migration by developing workload bundles and the appropriate migration sequence. Each bundle supports a single workload or a set of workloads supporting applications that do not have close dependencies on systems external to the bundle.

Using these tools and methodologies for discovery, validation, assessment, and planning should be highly automated and effectively orchestrated. Depending on your environmental complexity, a typical timeline for completing these activities is one to three months, which is far more efficient than other models.
1.3 Automated Rapid Migration

Your first step in executing Azure cloud migration is to establish network connectivity, cloud landing zone, and cloud management operations for incoming workloads. Azure cloud landing zone setup includes:

- Setting up accounts
- Virtual Private Cloud (VPC), network and security configuration
- Identity and access management roles
- Billing and invoicing, utilization and expense management
- Governance controls
- Shared services and tools (health and capacity monitoring, security controls, backup and disaster recovery/continuity of operations [DR/COOP], event and incident management systems, and integration)
- Container hosting platforms such as Azure ACI and container orchestration platforms such as Azure AKS

In your cloud management operations implementation, key processes must be deployed and teams mapped to support your cloud management. Unisys conducts project partnership workshops with you and other stakeholders to decide tooling and configuration preferences.

For optimum Azure migration results, you should consider the following essential processes:

1. Instantiate seed VMs in your destination Azure cloud: Wherever possible, use automation to collect detailed specifications from servers (physical and virtual) in the source environment and then create the VMs in the destination Azure cloud accordingly. This can be done through the APIs provided by Azure orchestration, or by simply creating “seed” VMs that will be replaced by the source server configuration or desired configurations during migration.

2. Back up the source workloads: You can create system state and data-level backup of the source workloads in a consistent state.

3. Move your backup files and data to the target cloud: You can move your backup files and data with encryption and compression to the target cloud either via network replication or by transporting them in a rugged physical appliance.

4. Restore and configure adjustment: At the Azure destination site, restore servers, applications, and data to the seed VMs already provisioned and apply source configurations to overwrite the seed VMs. You can apply proper device drivers based on the target Hyper-V and the migrated source workload operating systems. You also can set up new network configurations according to the network settings in the destination environment. All data are loaded into the appropriate cloud storage systems in the destination site automatically.

5. Replicate the incremental changes: Allowing normal production operation for the workloads in the source data center during migration lets you perform “incremental sync” that captures only data changes since a prior capture. It replicates incremental changes across your network to the destination site. The replication is compressed and encrypted. This greatly reduces the time needed and the impact on your source site systems.

6. Apply test and evaluation: The workloads migrated to your target cloud environment can be tested for application functionality, performance, and security. This evaluation can be performed with your existing application testing tools and scripts.

7. Cut over: After completing the last batch of incremental backup and restoring the servers from the backup, the cutover is performed. The servers in your target environment are promoted to production.

8. Perform post-cutover test and validation: Immediately after cutover, network connectivity and application functionality and performance, your supporting services (monitoring, security, backup and DR, etc.) are tested and validated.
You can install the Microsoft Migration service software as a virtual appliance in your secure environment with network access to both source data centers and the destination environment. It handles backup and replication across your network from the source data center to the target Azure cloud environment. [See Figure 1.]

Figure 1. Microsoft Migration Service from legacy to Azure
If the data and system backup size is too large for network transfer to be completed within a reasonable time, you can deploy a rugged portable system from Unisys with a form factor of flight carry-on luggage that includes compute capacity and 60+TB storage capacity. The device includes discovery software, migration software, and encryption capability. You can drop this “luggage” to a source data center for discovering and backing up workloads to be migrated and then shipped to the target cloud data center. This allows the cloud migration of large amounts of data and large systems to be completed in a much shorter time frame.

Other features and benefits you should look for include in a Azure migration solution include:

- **End-to-end migration management** with an intuitive user portal that facilitates migration planning and tracks and reports status.

- **Automated conversion** between different infrastructure platforms:
  - Handles migrations across a wide variety of virtualization platforms automatically, including Hyper-V, VMware, Kernel-Based Virtual Machine (KVM), etc.
  - Performs automated physical server to virtual server conversion.
  - Automates migration of VMware workloads to Azure, and private clouds built on Azure Stack.
  - Automatically accounts for the features and attributes specific to a given private cloud-build technology and performs transformation accordingly.

- **Agentless architecture** that avoids the need for you to install and manage agents in an environment with many servers. It eases operations and reduces your time, cost, and support efforts.

- **Support for cloud migration testing and validation.** This support allows you to stand up multiple systems in the destination site using a backup set before the final cutover.

- **Customized pre-capture, post-capture, and systems standing-up operations.** Scripted operations can be added to perform special actions before and after the image capture. Some examples include suspending virus scanning, putting an SQL database in backup mode before the capture, or changing the allocation of virtual resources during migration.

- **Highly efficient, resilient, and secure data transfer.** All data are transferred in encrypted and compressed format and secured from tampering or data pilferage. It provides error handling and operation retry features, so intermittent network connectivity issues do not cause data transfer failure.

- **Unwind logical volume management in physical systems.** In private and public cloud environments, storage subsystems are typically RAID configured. The Unisys solution automatically removes the logical volume management from physical systems contained in the source site during systems conversion.

- **Automated “guest software” management.** Many virtualization platforms require VMs to run platform-specific “guest software” (system software and drivers) to function properly. Our solution automatically removes the guest software from the source site images and applies the proper guest software required for the destination site.

- **Network configuration automation.** The network environment in the destination site often differs greatly from the source site. This feature automates the network setting reconfiguration and bulk editing for you to streamline the changes.

- **Right-sizing of applications.** Through this process, our solution also can determine the right size of the hosting servers in memory and processing. The added benefit for you is cost savings by knowing the right infrastructure is being used.
From configuration to capture to cutover, the Unisys end-to-end migration workflow turns what would be a complex migration process with unpredictable downtime into a series of simple and repeatable steps on groups of servers. You can replace numerous manual steps and eliminate a major source of migration errors and failures, while incorporating local customizations and special cases seamlessly into the process. With the Unisys workload migration solution, you will realize the following benefits:

- Rapid and secure migration for a large quantity of your workloads
- Near-zero disruption to production during your migration
- Automatic determination and execution of the required translation and transformation at the destination site; automatic handling of complex and error-prone transformations required to get your existing system running in a new infrastructure
- Support for all your virtualization technologies and bare-metal computers
- Automated customization supported before and after each stage of migration
- Management and tracking of migrations and all stages of each migration

After your migration, your organization can benefit from support provided through the Unisys cloud factory to help you get ready for operations in the Azure environment and optimize application performance in the cloud.

Unisys provides strong expertise and service experience in modernizing mission applications with cloud-native services, and PaaS and SaaS services. For example, we worked with the Georgia Technology Authority (GTA) to aid that state’s 10 million citizens during the COVID-19 pandemic. The Georgia Technology Authority, with Azure systems and support from Unisys, had the means and know-how to help citizens during the crisis in near real-time due to planning, foresight, and rapid deployment.

Some aid was highly visible, while other initiatives played out behind the scenes—but all were made possible by flexible, cost-effective Azure cloud systems engineered and deployed by Unisys.

Here are the top three rapid-response Azure cloud computing initiatives from GTA deployed this year:

- Microsoft artificial intelligence-driven chatbots quickly deployed on Georgia government Azure-based websites, delivering critical information to Georgia’s citizens, with over 16.5 million COVID-related queries answered.
- Quick deployment of secure, preauthorized Azure computing resources for every government agency in need of computing power to process unemployment claims, answer health and safety questions, and rapidly compile health information collected from the field. Vital resources were deployed in four hours or less—as opposed to the previous 12-month process.
- Azure-hosted resources deployed to agents in the field using inexpensive tablet-based devices to complete case work for citizens.
1.4 Azure Cloud Migration with DevSecOps

You should have the option to perform rapid and secure cloud migration with DevSecOps methodology and toolchains. This option is perfect for organizations that have adopted or started to adopt DevOps or DevSecOps continuous integration/continuous delivery (CI/CD).

With this approach, you can deploy configuration and orchestration management solutions, such as Puppet, Chef, Ansible, Terraform, etc., to capture the infrastructure and application configurations in the source data center and then deploy the configurations to the target cloud environment in the form of VMs, containers, or cloud-native services using DevSecOps methodology. You can use CI/CD tooling for application performance monitoring, test automation, configuration management, code vulnerability scanning, Section 508 testing, build repositories, and open source governance tools. You also can port the application artifacts (source code, test suites, build automation, test data, deployment automation) to the CI/CD toolchain. Landing zone templates can be used as part of your continuous delivery automation phase and incrementally build out a set of “infrastructure as code” artifacts in a time-boxed iterative manner.

This automation ensures that your application and associated content can be automatically and repeatedly (re)deployed with integrated regression, performance, and security scanning tests. You can leverage CI/CD tools that support dashboard (such as SonarQube, Synopsys, and Aqua Trivy) to automate the display of the current code quality and security quality of the application. The automated display minimizes the risk of out-of-date assessment documentation. With the Unisys solution, you have access to API management tools, such as OpenAPI (Swagger), to ensure documentation is up to date.

By applying the DevSecOps toolchain, you can automate cloud migration and continuous delivery of cloud applications. The choice of specific tools for your initiatives will be driven by many factors, including the consideration of tools you already deploy and use, standards and architecture, the unique requirements for migration, etc. You can make these decisions collaboratively with your service partner early in the cloud migration initiative.

1.5 Azure Hybrid Cloud-Enabled Networking

Virtualization of data center assets and growing reliance on hybrid cloud services are redefining the nature of enterprise-class networking. As your organization places more of its workloads in the Azure public cloud and adopts private cloud environments to serve the most critical business applications, you migrate away from hardware-based legacy networking models to software-defined networking models that accommodate your bandwidth, flexibility, and performance needs.

Your move to the cloud is not complete without cloud-enabled networking. This extends your network, at any data center gateway, with a secure private connection that enables a scalable and robust hybrid cloud networking infrastructure that delivers virtual instances of compute, storage, and network resources catering to both your public cloud services and business-critical private cloud applications.

The new data center needs a scalable and robust hybrid cloud networking infrastructure that delivers virtual instances of compute, storage, and network resources catering to several business-critical applications. However, these technologies must integrate and interoperate across data centers and applications that reside in multiple Azure clouds. Your organization must adapt to provide a safe, robust connection to business-critical applications and data while seamlessly enabling business users to leap into a fully digitized workspace.

Only a select few service providers like Unisys combine SDN, Network Virtualization, and Infrastructure-as-a-Service (IaaS) from various providers and deliver them as a single entity.
Many service providers offer SDN, Network Virtualization, and Infrastructure-as-a-Service (IaaS). But only a select few service providers like Unisys combine these services from various providers and deliver them as a single entity, eliminating the various interoperability and management issues that may occur if those services are delivered individually.

With a cloud-enabled network solution, you benefit from a seamless and secure connection across the WAN to remote data centers supporting both on-site and mobile connectivity. You enhance your network availability and security by offering dedicated connectivity from Unisys-hosted secure data centers using Multiprotocol Label Switching (MPLS) networks, Azure VPN Express, a Peer-to-Peer (P2P) Ethernet network, or cross-connects at our facilities.

### 1.6 Security Approval Acceleration and Secure Legacy Workloads

Even for rehost migrations, while there are no application changes, the security controls in the destination cloud environment still need to be set up and configured properly to meet assessment and accreditation requirements. Application updates/upgrades over time often lead to some deviation from the secure configuration compliance requirements and cause the security approvals for cloud migration to become a challenging issue that can cause long delays.

In addition, for legacy workloads (e.g., old operating systems, outdated software applications that cannot be patched) and specialized applications that cannot be patched easily (e.g., industrial control systems, medical control applications, enterprise resource planning [ERP] applications, scientific research applications), security compliance is a challenge when migrating to a multitenancy cloud environment. There are situations where applications need to be deployed across Azure clouds and on-premises data centers in a highly distributed architecture that is hard to secure.

To address these challenges, you should make certain you have: 1) Templated security control automation and secure configuration compliance automation; and 2) Security software that provides a compensating security control to protect legacy or distributed workloads.
1.6.1 Templated Security Control
Automation and Secure Configuration
Compliance Automation

Our solution automatically deploys required security controls and proper environmental configurations. It reuses and inherits the controls already authorized in the cloud compliance packages. We use Azure landing zones to isolate the controls to be addressed uniquely for each application in the migration. Our automation solution scans configuration compliance and applies security remediation for all workloads. It automates the creation and maintenance of secure, compliant Azure environments specific to each application. We offer preconfigured, templated security control solutions based on your organization’s security compliance requirements.

1.6.2 Secure Hybrid Legacy Workloads with Greater Security Requirements

Current methods, tools, and services for ensuring security and regulatory compliance of cloud infrastructures for high security may be inadequate, leaving these cloud users with few solutions to address their needs. With the Unisys security solution, you can implement continuous, real-time security posture management and regulatory compliance best practices for your Azure cloud and hybrid cloud environments.

You can secure your communities of interest from attacks by using the Unisys software-defined security solution that applies user identity, role-driven microsegmentation, and AES-256 encryption to protect data in motion. Our solution leverages role and identity of users and workloads, not by Internet Protocol (IP) addresses, to build security policies. It implements and manages a least privilege/zero-trust model based on identity and provides you with a unified security platform that can extend across the enterprise—cloud, data center, and mobile. Our solution is a National Security Agency (NSA) Commercial Solutions for Classified (CSfC) certified solution. It can be deployed over any network transports (physical or virtual) and effectively prevent unauthorized east-west network movement.

You will want to make sure your Azure cloud environments are:

- Preventing lateral movement of unauthorized users on your cloud network
- Minimizing exposure through identity-defined, securely encrypted communication
- Protecting legacy systems and workloads by reducing attack surfaces and confining user access and application traffic within a secured logical enclave
- Operating secure distributed applications across your public and private cloud environments
- Providing dynamic microsegmentation and quarantine threats in seconds instead of days or months

Use our CSfC security solution that supports any desired segmentation with highly flexible configurations. You can rapidly apply it to your target workloads and applications without any hardware purchase and deployment. The solution provides the security assurance to application owners and cloud hosting operators and enables a rapid and secure cloud migration.
1.7 Azure Cloud Management
Successfully completing workload migrations or application refactoring/recoding to the cloud is only half the battle. You still need to implement a cloud management service to ensure best practices are in place for enterprise-level service management, utilization and expense management, governance, and security. With Unisys, you can deploy multiple cloud management solutions for managing either hybrid cloud environments or Azure public clouds according to your needs.

Unisys cloud management solutions empower you to leverage a best practice framework for modernizing legacy infrastructure applications. You can conduct continuous assessments with remediation guidance on the best architecture and recommendations for migrating to the cloud and transforming applications. Infrastructure and application modernization guidance helps you update legacy software for modern business needs. You can review Azure Kubernetes Service security against best practices to ensure secure cloud deployment, management, and auto-scaling. And you can take advantage of Unisys partners such as Morpheus Data, which provides a powerful self-service engine for managing hybrid clouds and modernizing apps.

When you migrate to the cloud, it’s very important that cost optimization be a central part of what you do as you migrate and after you migrate. Even if you are able to successfully complete large-scale migrations, you may struggle to control costs over time as you accumulate overprovisioned or idle resources.

1.8 Migration Factory Project Approach Using Azure Migration Service
As you do your migration, you will want to consider a migration factory approach. This will give you migrations in Agile sprints in a highly repeatable manner across your multiple Azure sites in conjunction with Azure Migration Services, which enables you to perform migrations across multiple workload bundles or multiple data centers in parallel. Our migration factory concept of operations performs migrations in Agile sprints in a highly repeatable manner across your multiple Azure sites.

The migration factory project approach breaks down your migration into waves or phases in which servers, databases, and any other components for a group of applications can be moved to the cloud. The process creates parallel workflows and forms teams (called squads). Each wave can include multiple squads for server migrations, databases, etc. This process can be repeated with subsequent waves until completion of the migration.
2.0 SUMMARY

Utilizing a strategic and highly automated approach to your large-scale Azure migration gives you the following strategic advantages:

- Automated discovery and assessment; business unit-specific planning
- A repeatable “Azure migration factory” methodology that includes introduction of enterprise shared-service standards
- Agile-based planning/replanning migration management
- Continuous integration/continuous delivery (CI/CD) for DevOps/DevSecOps-enabled customers
- A migration management portal to track overall progress
- An end-to-end Azure cloud migration lifecycle that ensures optimal performance is maintained at the enterprise and application levels
- Comprehensive security and compliance

Unisys provides proven technologies, methodologies, processes, and expertise for large-scale Azure migration with desired speed and security. Our end-to-end fully automated Azure migration solution empowers you to move workloads in a managed, expeditious, and secure manner with near-zero down time and risk, realizing high return on your investment.

Our solutions address the full life cycle needs of your Azure cloud adoption and service management. Unisys expertise in applying Microsoft Cloud Native services, PaaS, and SaaS solutions to modernize applications and transform IT allows you to maximize the value of Azure cloud adoption.

For more information, go to Unisys.com/cloud.