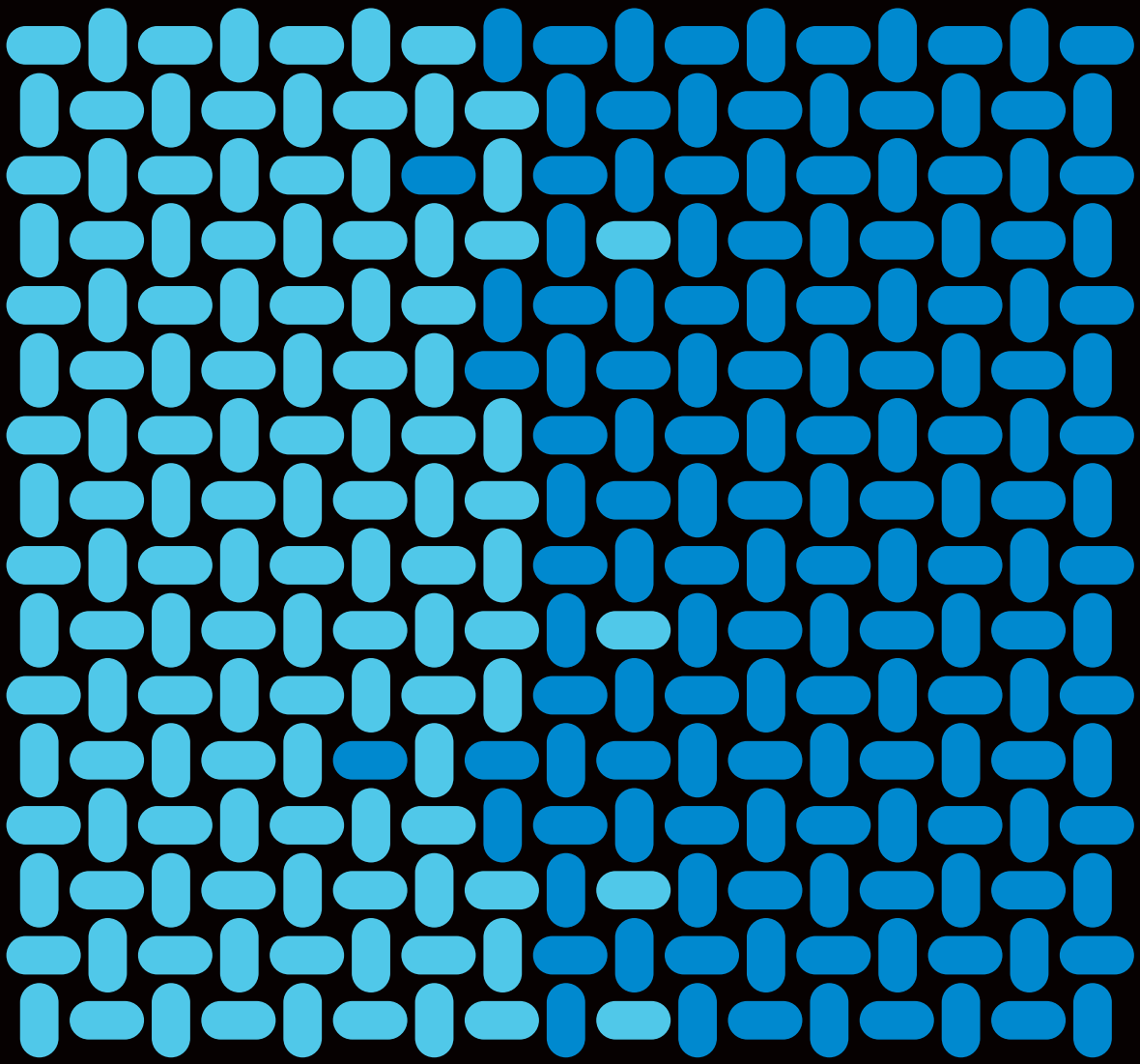
Azure e-book series

Microsoft

Moving Windows Server to Microsoft Azure to enable compliance



Contents

01 Introduction

Enterprise datacenters have been running on Windows Server for more than two decades. From Windows NT Server to Windows Server 2019, organizations have trusted the reliability, compatibility, and security of Microsoft server operating systems to handle their mission-critical applications and services in on-premises datacenters.

> **Azure provides over 90 compliance offerings specific to various countries, regions, and industries.**

Today's demands on computing resources are much more complex, and many companies are making a move to the cloud to take advantage of cost saving and convenience benefits. In addition, there is another important reason to consider migrating on-premises services to the cloud. More and more business sectors are operating under some degree of government and/or industry regulation. Navigating the maze of compliance requirements is time consuming and expensive. The right cloud provider can help you meet that challenge.

Security and data privacy are key elements of compliance. Data breaches cost organizations millions of dollars per year. Ponemon Institute's 2019 report[1] on the cost of a data breach set the average global total at almost $4 million USD, with the average in the United States coming in at over $8 million. Even more troubling was the finding that it took organizations an average of 279 days to detect and contain a breach, thus potentially exposing thousands of personal data records to compromise and exposing the organizations themselves to financial, reputational, and legal consequences.

Government and industry regulations are aimed at helping prevent data breaches and protecting the privacy of personal information. Azure provides over 90 compliance offerings specific to various countries/regions and industries. The Azure platform meets some of the most rigorous security and compliance standards in the world. Azure also provides governance, risk, and compliance tools along with guidance documentation to help you develop your own compliant cloud apps and document your adherence to compliance standards. With Azure Blueprints, Azure Policy, built-in compliance controls, configuration management tools, implementation and guidance resources, and third-party audit reports, Microsoft does much of the work for you so you can focus more of your efforts on your core business processes.

A major migration is a multi-phased undertaking that demands careful assessment and preparation. It begins with the design of a migration strategy that meets your business needs, including compliance requirements. This document is designed to help you understand how Azure can facilitate regulatory compliance for your organization's IT operations and provides guidelines for planning a migration from an existing Windows Server environment to the Azure cloud with a focus on meeting and maintaining compliance standards and goals.

1. Ponemon Institute, Cost of a Data Breach Report 2019, IBM Security, July 2019.

Take-away

Azure can facilitate regulatory compliance for your organization's IT operations when you migrate from an existing Windows Server environment to the Azure cloud.

02
Making the move: Migration overview

The Gartner Group predicted[2] that the public cloud services market will reach over $213 billion in 2019, with exponential growth expected through 2022. Forbes says 83% of enterprise workloads will be in the cloud by 2020. Microsoft continues to report healthy growth rates for Azure offerings as more and more enterprises as well as midsize and small businesses move their applications and services to the Azure cloud.

2. Sid Nag, Forecast: Public Cloud Services, Worldwide, 2016-2022, 4Q18 Update, Gartner Research, April 2019.

Thousands of companies move to the cloud every year. Successful migration is built on a plan that will help you determine the optimal platform and priorities for running business applications, create the initial technical plans and business justification, ensure your workloads will run as expected, and perform the migration with limited impact on the business.

Is migration worth the cost and effort? According to the IDC white paper titled *Microsoft Azure is Helping Organizations Manage Regulatory Challenges More Effectively*,[3] organizations in the United States. that use Azure to optimize their regulatory compliance initiatives reported an average 465% return on investment with six months to payback, while fundamentally improving key aspects of their compliance operations.

Migration tools

Regardless of how simple or complex your configuration is, how many servers and virtual machines (VMs) you need, and the applications on which your business processes depend, the right tools and processes can help expedite your migration program and help ensure that it proceeds smoothly. Azure provides tools and recommends third-party solutions that enable you to automate parts of the migration process.

- **Azure Migrate** provides a free central hub for starting, executing, and tracking your Azure migration. It helps you discover, assess, and migrate your on-premises applications, infrastructure, and data, including on-premises VMware or Hyper-V VMs as well as your physical Windows Server servers.
- **Azure Cloud Adoption Framework (CAF) Blueprint** helps you to create a migration "landing zone" that is provisioned and prepared to host workloads being migrated from your on-premises environment into Azure, which can be customized to fit your compliance needs.
- **Azure Site Recovery** enables you to replicate and migrate your VMs to Azure using right-sizing recommendations for migration as part of the assessment phase, and you can take advantage of Azure Hybrid Benefit when the initial replication occurs (as a configuration option). This saves you time, as you don't need to retroactively go back and perform these tasks for each VM.
- **Azure Database Migration Service** can be used to migrate your existing application database to Azure as a VM, as an Azure Managed Instance, or directly to Azure SQL Database, using a simple, self-guided migration process.
- **Azure migration partner tools** are ready-to-use partner solutions that have met our highest standards and can help you plan and migrate to the Azure cloud with fully managed services that assist in optimizing and securing your environment.

The Azure Migration Center is a web-based repository where you can find tools, resources, and guidance to make your migration journey easier.

3. Ryan O'Leary and Harsh Singh, Microsoft Azure Is Helping Organizations Manage Regulatory Challenges More Effectively, IDC, May 2019.

03
Regulation considerations: Compliance overview

Some industries, such as healthcare and financial services, have been subject to government oversight impacting IT processes for many years. Now more business sectors are falling under the reach of the regulatory arm, with broad privacy laws such as the European Union's General Data Protection Regulation (GDPR) that became enforceable in 2018, the state of California's Consumer Privacy Act (CCPA) that takes effect in 2020, and many others around the world that are impacting organizations in all business sectors.

Today almost every business is subject to regulatory mandates. For example, the GDPR applies to organizations outside the EU if they offer goods or services (including free ones) to any resident of the EU. The regulatory landscape is constantly evolving and expanding, and the complexity of achieving and maintaining compliance increases in the process. This means cloud providers and cloud customers must adhere to broad security standards, such as data classification, access management, encryption, logging and reporting, security incident response, and so forth.

The cost of compliance

The cost of compliance can be steep. Ernst & Young estimated[4] that the world's five hundred largest corporations would spend a total of $7.8 billion on GDPR compliance alone. This includes spending on legal fees, consulting fees, new technology, and hiring of new personnel.

However, the cost of non-compliance can be even higher. The Ponemon Institute report titled *The True Cost of Compliance with Data Protection Regulations*[5] found the cost of non-compliance to be 2.71 times the cost of compliance. Fines for violations under the GDPR can reach €20 million or 4% of an organization's entire global turnover for the preceding fiscal year. In addition, failure to comply can result in damage to reputation, loss of revenues, and business disruption.

Achieving and maintaining compliance

Moving your applications and data to the cloud can help reduce the costs of compliance, but successfully completing your migration to Azure is only the first step. Once your resources are residing in the cloud, you must take further steps to ensure ongoing compliance and keep those resources accessible to those who need them. Microsoft provides additional tools to help you with that. These tools are in addition to the security and compliance frameworks built into the Azure infrastructure, both of which we'll discuss in more detail in the following sections.

4. Jeremy Kahn, Stephanie Bodoni, and Stefan Nicola, It'll Cost Billions for Companies to Comply with Europe's New Data Law, Business Week, March 2018.

5. Ponemon Institute, The True Cost of Compliance with Data Protection Regulations, Globalscape, December 2017.

04
Compliance in the cloud: The Azure advantage

As documented in its report, *Microsoft Azure is Helping Organizations Manage Regulatory Challenges More Effectively*, IDC interviewed organizations that are using Azure as a platform to optimize their regulatory compliance initiatives, with special emphasis on survey data derived from government, healthcare, and financial sectors. Based on the data gathered, IDC found that these organizations are realizing significant benefits by leveraging Azure capabilities to make their regulatory and compliance efforts more effective while doing so in a secure and cost-effective manner.

According to IDC calculations, the organizations surveyed will realize annual benefits worth $4.29 million per organization. This includes not only the value of risk mitigation and business benefits, but also IT staff productivity gains and IT infrastructure cost reductions. Advantages of migrating to Azure include security and governance, scalability, availability, flexibility, agility, convenience, cost savings, and of course, compliance.

Azure secure infrastructure

The Azure infrastructure is built with stringent digital and physical security controls that help protect against attackers and intruders and help protect the privacy of data as required by government and industry regulations. Microsoft has the resources to invest in the best state-of-the-art security technology and talent.

Azure datacenter facilities have extensive layers of physical security and strict access policies. Microsoft employs more than 3500 cybersecurity professionals and uses advanced analytics to link massive amounts of threat intelligence and security data and provide unparalleled threat protection and detection. The Azure cloud is continuously monitored by Microsoft, making it difficult for an attacker to penetrate.

Take-away

According to IDC's white paper, organizations in the United States that use Azure to optimize their regulatory compliance initiatives reported an average 465% return on investment with six months to payback, while fundamentally improving key aspects of their compliance operations.

Azure compliance and security toolset

The Azure compliance and security toolset builds in control-mapping capabilities, workflow management tools, and audit functionality and helps you implement compliance using such products, features, and services as:

- **Azure Blueprints** helps customers build Azure applications that are secure and comply with many regulations, including the GDPR and HIPAA, both internally and externally. They also simplify large-scale Azure deployments by packaging key environment artifacts, such as Azure Resource Manager templates, resource groups, role-based access controls, and policies, in a single blueprint definition. You can use blueprints provided by Microsoft such as the Cloud Alliance Framework (CAF) blueprint and the ISO 27001 blueprint, customize the built-in blueprints, and create your own blueprints.
- **Azure Policy** helps define and enforce policies that aid in making the Azure environment compliant with internal policies and external regulations.
- **Azure governance** helps enforce and audit your policies for any Azure service and ensure that you're compliant with external regulations by using built-in compliance controls.
- **Azure regulatory compliance dashboard** provides insight into the compliance posture for a set of supported standards and regulations, based on continuous assessments of the Azure environment.
- **Azure Security Center** provides unified security management and advanced threat protection across hybrid cloud workloads. The Security Center enables you to take advantage of such capabilities as centralized policy management, continuous security assessment, actionable recommendations, and advanced cloud defenses, as well as prioritized alerts and incidents and integrated partner solutions.
- **Azure Sentinel** a scalable, cloud-native security information and event manager (SIEM) platform that uses built-in AI to analyze large volumes of data across the enterprise from all sources. It includes built-in connectors for easy onboarding of popular security solutions and allows you to collect data from any source with support for open standard formats.
- **Data protection** helps keep data private and protected with such features as virtual machine disk encryption for both Windows and Linux VMs, virtual machine backup with Azure Backup, Azure Information Protection to help classify and protect documents and email by applying labels, Microsoft Cloud App Security to protect sensitive files in the cloud, and cloud disaster recovery with Azure Site Recovery.
- **The Service Trust Portal** helps with self-service audits and compliance by providing deeper technical trust, security, privacy, and compliance information.
- **Compliance Manager** enables you to track, assign, and verify your organization's regulatory compliance activities related to Azure and Microsoft cloud services, and provides a compliance score to help you track your progress and prioritize the auditing controls that will help reduce exposure to risk.

Azure compliance benefits

The IDC study participants reported that Azure helped them better manage spikes in the workload, enabled faster access to and analysis of data during audits, and reduced exposure to risk based on the strong internal controls of Azure, while saving time and keeping costs in check.

Additional specific benefits of migrating to Azure in regard to compliance include:

- Shared responsibility to relieve some of your security and compliance burden
- Enhanced currency and updatability in response to changing standards
- Scalability to meet the needs of changing environments
- Governance to provide strategic direction and a framework for security implementations
- Control mappings to required security standards
- Improved speed and agility for compliance auditing and reporting
- Improved data management capabilities

We'll discuss each of these in more detail in the following sections.

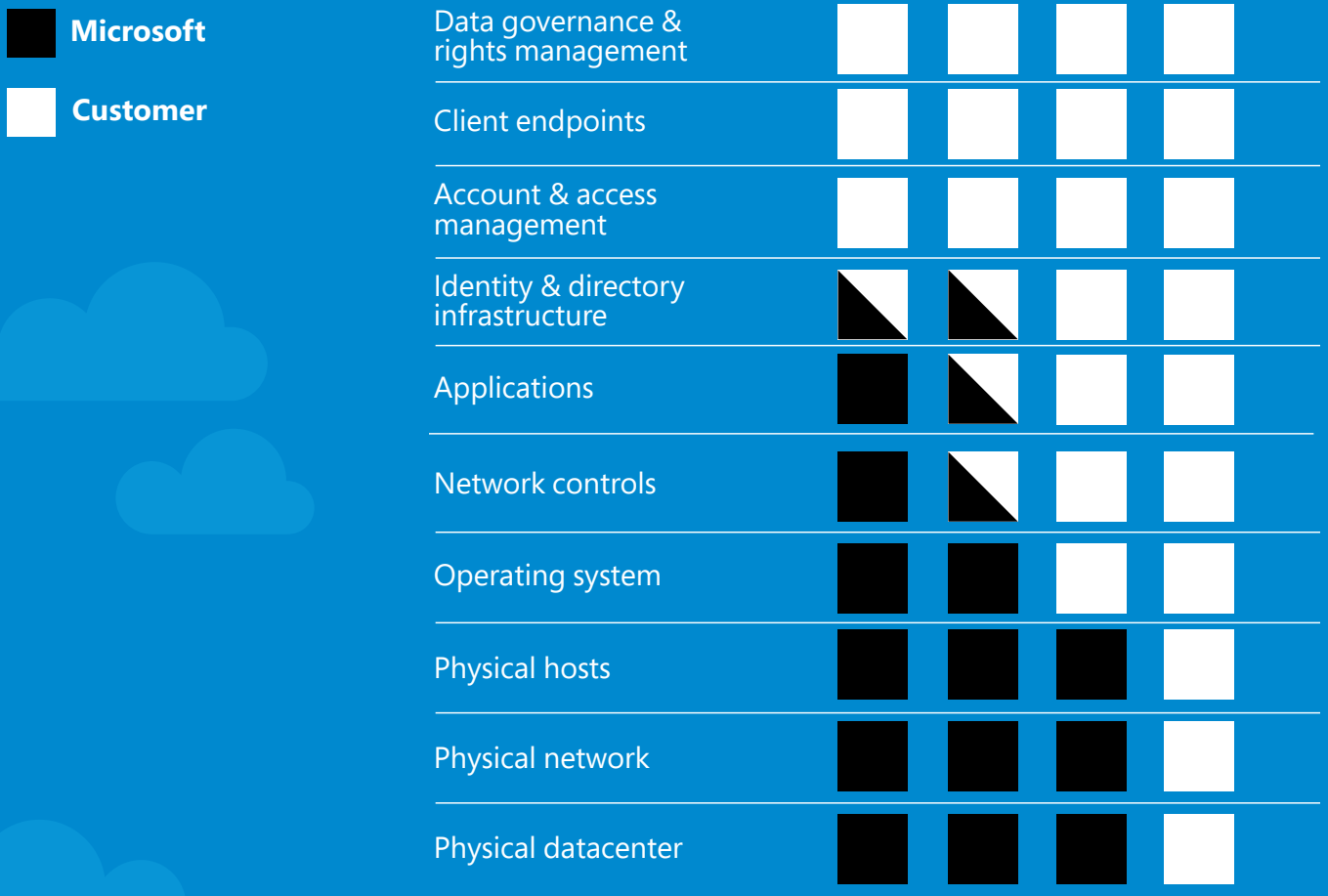
Take-away

The Azure compliance and security toolset builds in control-mapping capabilities, workflow management tools, and audit functionality and helps you implement compliance.

Shared responsibility

When your organization's IT operations run in an on-premises datacenter, security and compliance fall squarely on your shoulders. Physical security, host infrastructure, and network controls are wholly your responsibility. When your resources reside in the cloud, security becomes a responsibility that's shared with the cloud provider. While you will still be responsible for many aspects of security, Microsoft becomes responsible for others, depending on the applicable cloud computing model.

In the context of moving your production servers and data to the cloud, Azure is based on the infrastructure as a service (IaaS) model. In this model, as illustrated in the chart below, Microsoft bears full responsibility for the physical security of the host servers and the datacenter's network on which your virtual machines run.



When you run your servers on premises, keeping current on these changes can be a daunting challenge. In the Azure cloud, thanks to the shared responsibility model, you can trust that the underlying platform is being continually updated by Microsoft to make it more secure and to roll out new security features.

You retain responsibility for the security of the guest operating systems running on your VMs, applications, user accounts and identity, and access and network controls. In addition, you are responsible for the security of your client endpoints and for the protection of your data.

A thorough understanding of this shared responsibility model is essential to meeting your compliance goals when you migrate to the Azure cloud. You can use tools such as Azure Blueprints to ensure that those goals are consistently met across all of your areas of responsibility.

When using Azure as a development platform (PaaS) or using an Azure-based software service such as Office 365 (SaaS), the distribution of responsibilities will differ.

Enhanced currency and updatability

Compliance requirements are constantly changing, and the security landscape frequently shifts as attackers utilize new methods against which you must defend. Old methods can fall behind the curve as new threats require innovative solutions. Agility in responding to a frequently changing landscape of state, national, and international regulations is critical to avoid compliance-related penalties.

When you run your servers on premises, keeping current on these changes can be a daunting challenge. In the Azure cloud, thanks to the shared responsibility model, you can trust that the underlying platform is being continually updated by Microsoft to make it more secure and to roll out new security features. You can find announcements and information about these in the Azure Blog Security section.

You are still responsible for operating system and application updates, but Microsoft helps make it easier. The Azure Update Management solution in Azure Automation, which is included with your subscription, helps you assess the status of available updates across both Windows and Linux VMs and easily manage the process of installing needed updates.

Azure Security Center monitors Windows and Linux virtual machines (VMs) and computers daily to detect missing operating system updates. Security Center retrieves a list of available security and critical updates from Windows Update or Windows Server Update Services (WSUS) and checks for the latest updates in Linux systems. If a VM or computer is missing a system update, Security Center will recommend that you apply system updates and give you the option to implement the recommendation. The dashboard provides you with information regarding the severity of each of the missing updates.

Azure Blueprints can help you keep your environment up to date by easily updating a blueprint assignment to a newer published version and tracking blueprint versions to push updates.

> Azure Blueprints make it easier to achieve governance at scale, with the ability to deploy blueprints to multiple Azure subscriptions with a single click and manage all your blueprints from a central location.

Scalability

As your organization grows, some security and privacy solutions that may have worked on a small scale can become unwieldy or completely unworkable, resulting in a compliance gap. Operations that can be handled manually at one stage of a company's lifecycle, such as responding to requests of data subjects, may become overwhelming unless properly automated. A scalable compliance strategy remains both efficacious and cost-effective as your organization changes in size and scope of business.

A major advantage of the Azure cloud over an on-premises datacenter is scalability, and this becomes even more important in regard to regulatory requirements. Azure is designed to easily scale to fit the capacity of your current workloads automatically, using the Azure Autoscale feature that is built into cloud services and virtual machines. Azure compliance tools are designed to help you meet privacy, security, and transparency regulations as scale changes, dynamically adjusting to fit an expanded or contracted infrastructure. Many security-related processes, such as monitoring update compliance and tracking configuration changes, can be automated for better efficiency and scaling using Azure Automation.

Azure Blueprints makes it easier to achieve governance at scale, with the ability to deploy blueprints to multiple Azure subscriptions with a single click and manage all your blueprints from a central location.

Because compliance involves not only the implementation of appropriate security measures but also auditing and reporting to document adherence to the rules, these aspects must also be scalable to accommodate changes in your environment. Azure auditing and reporting solutions can facilitate compliance at every stage of deployment and operation.

Governance

Cloud governance provides the framework for your security implementations, by providing strategic direction for the people, processes, and technologies that are responsible for keeping your cloud data private. Azure simplifies the governance process and helps you map policies to security standards for compliance using Azure Blueprints.

Governance principles and practices

In the cloud, governance involves the process by which your IT policies are devised, set, maintained, enforced, monitored, and audited. Governance for compliance helps ensure that your standards and policies are consistent with the best practices that prevail in your industry and are mandated by applicable regulations.

Governance is driven by policy, and in the context of compliance, this means security and management policies. One of the biggest challenges in cloud governance is ensuring consistency in the deployment of cloud policies, access controls, and resource configurations.

When you migrate from an on-premises environment to Azure, you need to be able to easily set up compliant foundational architectures. Azure Blueprints and Azure Policy help you to accelerate the migration process by simplifying the deployment of a fully governed landing zone.

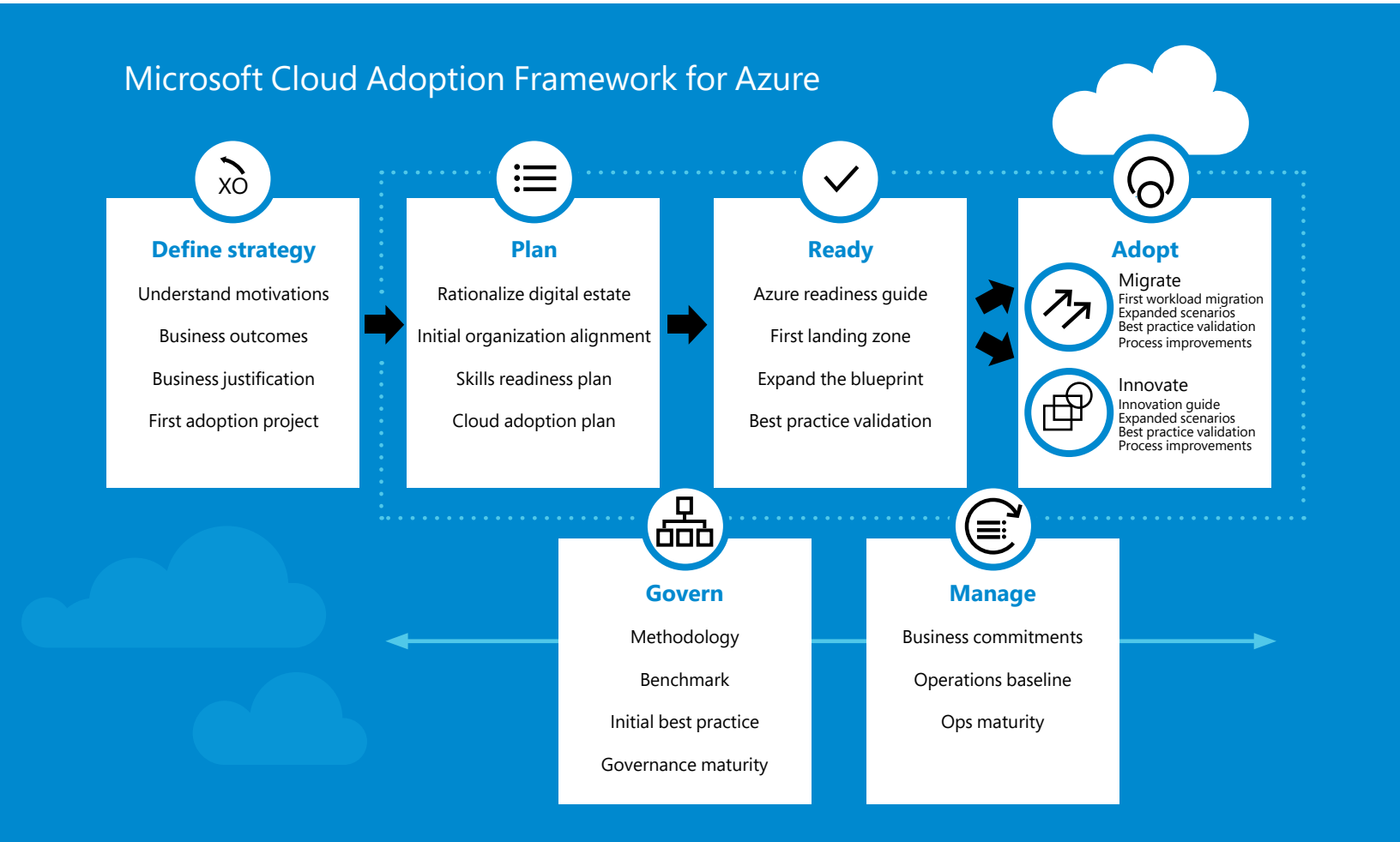
Azure Blueprints overview

In its traditional sense, a blueprint is a design plan or schematic, created by architects and engineers to help construction workers build structures to consistent standards and comply with building codes.

Azure Blueprints is a free service that provides you with templates to create, deploy, and update fully governed cloud environments to consistent standards and comply with regulatory requirements. Azure Blueprints do not replace Azure Resource Manager (ARM) or Azure Policy; rather, it is a package that contains different types of components—including ARM templates, policy assignments, resource groups, and role assignments—all in one container, so you can quickly and easily deploy all these components, which are called artifacts, in a repeatable configuration.

Blueprints give you greater scalability, easier updatability, and more flexibility than ARM templates alone. Blueprints exist natively in Azure, unlike ARM templates, and can be saved to management groups or to an Azure subscription (with Contributor access). Thus, Blueprints support better tracking and auditing of deployments.

You can use the built-in blueprints or create your own custom blueprints. Blueprints can be created in the Azure portal or using the REST API with tools such as PowerShell. If the latter method is used, you can define blueprint parameters to prevent conflicts when reusing certain blueprints.



> Security controls are central to most compliance offerings. Azure Blueprints can map security controls to specific compliance requirements so you can apply them to your Azure environments easily and consistently.

Built-in blueprints. Microsoft provides built-in blueprints to help you with common deployment scenarios. The CAF blueprint builds a foundation or "landing zone" for your migrated resources that serves as a starting point. The CAF blueprint deploys migration tools, provisions operational workspace and diagnostic storage accounts, and creates a virtual network with subnets for gateway, firewall, jumpbox, and landing zone.

The CAF is intentionally limited. It is designed for a single production subscription and assumes that no Azure policies are to be applied and no third-party compliance requirements are needed. The blueprint can be extended to create a landing zone blueprint that fits your organization's needs.

You can layer standards-based blueprints on the CAF to meet your compliance requirements. Microsoft provides several built-in blueprints to deploy common compliance certification standards. For example, the ISO 27001 blueprint and the PCI DSS blueprint map a core set of policies for those respective standards to any Azure environment. Blueprints can be deployed to multiple Azure subscriptions, managed from a central location, and are scalable to support production implementations for large-scale migrations.

Resource locking. Azure Blueprints support resource locking, by which you can maintain consistency once you've created a compliant environment. The blueprint assignment can be set to one of three modes: Don't Lock, Read Only, or Do Not Delete. Artifact resources can be in one of four states: Not Locked, Read Only, Cannot Edit/Delete, or Cannot Delete. The blueprint lock cannot be removed outside of Blueprints.

Azure policy. Meeting compliance requirements starts with creating rules to govern your IT operations but enforcing those rules continuously and consistently can be a challenge unless you automate that enforcement through the application of policies. Azure Policy is a service that you can use to create, assign, and manage policies to enforce different rules in relation to your resources so those resources will stay compliant with your corporate standards and regulatory requirements. Azure Policy focuses on resource properties; it controls such properties as the types or locations of resources.
Azure policies can be included as an artifact in a blueprint to ensure that only approved or expected changes can be made to the environment to protect ongoing compliance with the intent of the blueprint.

Security and privacy

Compliance requirements are generally aimed at protecting the privacy of personal data, and without security there can be no privacy. To understand the difference between the two, think of privacy as the objective and security—in the context of compliance—as the means by which you attain that desired result. Although it may seem counterintuitive, moving your data out of your private datacenter to the Azure public cloud can result in increased security that enhances the privacy of that data.

Microsoft takes a defense-in-depth approach to security in Azure, working together with customers and combining built-in security controls and partner

Defense in Depth | Microsoft and Partners				
Identity & Access	**Apps & Data Security**	**Network Security**	**Threat Protection**	**Security Management**
Role based access	Encryption	DDoS Protection	Antimalware	Log Management
Multifactor 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

solutions to help you comply with security requirements.

Security controls are central to most compliance offerings. Azure Blueprints can map security controls to specific compliance requirements so you can apply them to your Azure environments easily and consistently.

The Azure multi-layered security strategy addresses compliance requirements at all levels:

- Physical infrastructure
- Platform security
- Secure software development
- Network security
- Virtual machine security
- Application security
- Data security

Let's take a closer look at each of these.

Physical infrastructure

Microsoft is responsible for securing the physical servers and the cloud platform. Toward that end, the Azure cloud is built on a foundation of state-of-the-art multi-layered security. This begins at the physical level. Azure datacenters deploy ISO-compliant safeguards and the Azure Operations Team

> The Azure platform is designed to provide a trustworthy foundation, documented through multiple levels of monitoring, logging, and reporting and access controls.

uses hardened administrator workstations for connecting to and managing Azure infrastructure components. Staff members undergo annual security and privacy training including secure operations, safe data handling practices, and standards of conduct.

Platform security

The Azure platform is designed to provide a trustworthy foundation, documented through multiple levels of monitoring, logging, and reporting and access controls. Azure uses logical isolation to segregate each customer's data from the data of others and prevent customers from accessing one another's data. Microsoft follows strict standards for overwriting storage resources when customers delete data or leave Azure, and decommissioned hardware is physically destroyed according to NIST 800-88 guidelines.

Secure software development

The Security Development Lifecycle (SDL) is used internally to help ensure that Microsoft products and services such as Azure are highly secure and address security compliance requirements. Security and privacy considerations are a focus throughout all phases of the software development process.

Network security

Azure virtual networks (VNets) on which your Azure VMs and network devices run provide logical isolation of the Azure cloud network dedicated to your resources so you can securely connect Azure resources to one another. VNets can be connected to your on-premises networks. Azure also supports a dedicated WAN link between your VNets and your on-premises network with ExpressRoute. Site-to-site and point-to-site virtual private networks (VPNs) can securely connect on-premises devices to resources on your Azure VNet.

Azure Blueprints can create a complete networking setup configured to your specifications. Setup of a virtual network is included in the CAF blueprint by default. Networking design decisions will be an important part of your migration plan.

Authentication and authorization. The first step in protecting network resources is strong authentication to ensure that only those with legitimate credentials can gain access. Azure Active Directory provides an identity infrastructure and enables you to verify every identity with conditional access and Zero Trust. You can help keep users compliant with Azure AD access reviews. Azure Multi-Factor Authentication provides an added layer of protection and helps safeguard access through a two-step verification process that helps prevent remote attacks even when credentials are compromised.

The CAF blueprint assumes that the Azure subscription is already associated with an Azure Active Directory instance. Microsoft recommends that you treat identity as the primary security perimeter and integrate your on-premises and cloud directories to centralize identity management.

Access controls. Azure supports several types of network access controls. You can filter traffic using Network Security Groups (NSG) and use virtual network security appliances to provide such services as virtual firewall, intrusion detection and prevention, or multifactor authentication. Azure Traffic Manager enables you to control the distribution of traffic across your application endpoints.

Azure utilizes role-based access control (RBAC) to resources on virtual networks. Azure Security Center can manage the NSGs on VMs and lock access to a VM until a user with the appropriate RBAC permissions requests access. Azure Policy enables you to create, assign, and manage policy definitions. Policy definitions enforce different rules over your resources, so they stay compliant with your organizational standards. You can use forced tunneling and user defined routes (UDR) to ensure that your services are not allowed to initiate a connection to devices on the internet.

Azure Blueprints enable you to deploy RBAC assignments as artifacts within a blueprint. Role assignments can be defined for the entire subscription or nested to a specific resource group included in the blueprint.

Virtual machine security

Azure enables you to deploy VMs running Windows or Linux and easily govern, secure, monitor, and back up the VM environments to help ensure compliance. By default, VMs inside the private network do not receive inbound traffic from outside of the deployment.

For even more security at the host level, you can deploy your Azure VMs on Azure Dedicated Host, a physical server used only by your organization. Under the shared responsibility model, you are responsible for the security of the VM operating system, but Microsoft provides tools to help, including Azure Security Center, Microsoft Antimalware for Azure, Azure Advisor, Azure Backup, and Azure Monitor. Azure Blueprints can help protect your virtual machines by consistently applying security and compliance controls through Azure policies.

Application security

Vulnerable software applications put the network and data at risk. Applications are responsible for more vulnerabilities than operating systems or hardware, so securing the apps that run in your Azure cloud is vital to meeting compliance requirements. Microsoft provides features and tools to help you make and keep applications secure, including sample apps, best practices, and secure development guidance.

Azure provides a platform-as-a-service (PaaS) solution for developing and hosting your own secure applications. Azure App Service, which is ISO, SOC, and PCI compliant, can secure your web apps and mobile back ends. Azure Security Center helps monitor and protect your applications running on top of App Service. Microsoft Security Risk Detection is a cloud-based tool that you can use to detect bugs and other security vulnerabilities in your software before you deploy it to Azure.

> Azure supports various encryption models, including server-side encryption that uses service-managed keys, customer-managed keys in Key Vault, or customer-managed keys on customer-controlled hardware.

You can register your applications with Azure Active Directory to use its authentication and authorization services to control access to application resources.

Microsoft Cloud App Security is a Cloud Access Security Broker (CASB) that operates on multiple clouds, including Azure, to help prevent data leaks to non-compliant apps and limit access to regulated data.

Within your Azure VNets, Application Security Groups (ASGs) enable you to define fine-grained network security policies based on workloads, centralized on applications instead of explicit IP addresses. You can isolate workloads and protect them individually so that if a breach occurs, it limits the potential impact of lateral exploration of your networks by hackers.

Data security

In the context of privacy compliance, ultimately it's all about protecting the data. When your organization collects, stores, and/or processes the personal identifiable data of customers, employees, or others, you incur obligations to protect the privacy of that information whether it resides in your on-premises network or in the cloud. A comprehensive and integrated compliance strategy will involve defining specific measures applicable to all organizational processes and personnel that handle personal data.

The data you store in the Azure cloud belongs to you. Your organization owns and controls the collection, use, and distribution of its information. The Microsoft Privacy Statement puts this commitment in writing and details Microsoft data protection policies and practices. Azure administrators or support staff are provided with just-in-time access to customer data when needed, and it is revoked when no longer necessary.

It is important to understand the types of threats that apply to your data – unauthorized access/exposure, loss/deletion, misuse, tampering or alteration – as well as the level of risk (how likely to occur) and the severity of the potential consequences. Data threats can come from internal or external sources and can be deliberate or accidental, which may call for differing preventative and response measures.

Encryption. Encryption of personal data can help protect it in case of a breach. Azure supports various encryption models, including server-side encryption that uses service-managed keys, customer-managed keys in Key Vault, or customer-managed keys on customer-controlled hardware. Azure includes data protection capabilities via built-in services, components and configurations that apply encryption to internal data and traffic. Some are enabled by default and others you can choose to enable.

You can use encryption technologies built into or supported by Azure to encrypt personal data at rest, in transit, and in process. Azure Blueprints can apply policies on the use of cryptographic controls and ensure that information transfer with Azure services is secure.

Document protection. Personal data can reside in email and documents, and a good compliance strategy requires that you identify and protect this information. Azure Information Protection is a cloud-based solution that helps you classify, label,

and protect your organization's documents and emails with embedded labels and permissions, using Azure Rights Management to stay in control of how data is accessed, used, and distributed even when it's shared with other people.

Confidential computing. Azure confidential computing is aimed at protecting the confidentiality and integrity of your data as it's being processed in the cloud. This adds new data security capabilities using trusted execution environments (TEEs), which are hardware or software implementations that safeguard data being processed from access outside the TEE.

Agile auditing and reporting

Auditing is a crucial part of your compliance strategy and the Azure environment is audited continuously. Auditing helps you determine whether your organization is meeting regulatory requirements, identify deviations, and rectify them. Cloud-based compliance auditing offers such benefits as:

- Easier access to audit data
- Better management of data for privacy assurance
- The ability to use Azure tools that help simplify the process
- Better logging and documentation

Azure provides a wide array of security auditing options, with authenticated and trustworthy logging of security-relevant events that generates an audit trail and is engineered to be resistant to tampering. You can use comprehensive and configurable logs and logging tools to track and record activities to document compliance.

- **Azure Active Directory** produces logs that track sign-in activity and application usage.
- **Azure Diagnostics** provides a view of core analytics.
- **Log Analytics** can aggregate and analyze Windows Event logs, IIS logs, and Syslogs for Windows and Linux machines.
- **Azure Monitor** enables you to track API calls in customers' Azure resources.
- **Azure Security Center** provides you with tools to collect and review security logs from across Azure applications and services, including the regulatory compliance dashboard.
- **Azure Storage Analytics** can trace data requests made against Azure Storage.

You can use Compliance Manager to combine detailed compliance information Microsoft provides to auditors and regulators about its cloud services with your compliance self-assessment for standards and regulations applicable to your organization. Compliance Manager can produce richly detailed Microsoft Excel reports that document compliance activities performed by Microsoft and your organization for auditors, regulators, and other compliance reviewers.

If your organization uses Office 365, you can view user sign-in reports, user activity reports, and the Azure Active Directory audit log in the Security and Compliance Center, along with Exchange and SharePoint Online audit reports.

> Azure provides tools that make it easier for you to respond to and address data subject requests in a timely manner as required by regulations such as the GDPR.

For audit reports on the Microsoft cloud services, including Azure, you can use the Microsoft Service Trust Portal.

Improved data management

Data management is a very broad subject. It includes developing a governance plan, defining policies, and applying those policies to the data you collect, process, and store. Azure provides tools for managing data in a secure and compliant manner.

Azure can help you with consent management, notification documentation, and automating the security measures that keep data private. The Azure infrastructure can host customized privacy notices to help meet GDPR notification requirements. Azure Active Directory enables requesting and obtaining consent to use of data, and Azure SQL Database can be used to document data subjects who have granted their affirmative consent.

Data discovery, identification, and classification

The first step in meeting data privacy obligations under many regulations is to locate and identify all personal data that is being stored or managed by your organization. Azure provides you with tools that you can use to search for personal data in your Azure environment.

These include Azure Search, Azure Data Catalog, Azure Active Directory, and Azure SQL Database. You can use Power Query in Excel to find data associated with Hadoop clusters in Azure HDInsight after importing it. You can use Query Explorer to find data stored in Cosmos DB.

Classification of data, so you can assign the 13 appropriate controls to comply with applicable data protection requirements, can be accomplished using Azure Information Protection and Azure Data Catalog. You can use AIP labels to classify documents and email, which makes the classification identifiable regardless of where the data is stored or with whom it's shared. Data sources that are registered with Azure Data Catalog can be annotated manually or using the REST API in accordance with your classification standard.

Data subject requests

An important aspect of managing personal data in compliance with privacy regulations involves responding to the requests of data subjects to provide them with copies of their data, to correct inaccurate data or rectify incomplete data, and in some cases to restrict the processing of their data or erase it.

Azure provides tools that make it easier for you to respond to and address such requests in a timely manner as required by regulations.

Data subject requests are executed within a given Azure Active Directory tenant. Microsoft provides the ability to access, delete, and export certain customer data through the Azure Portal and also directly via pre-existing application programming interfaces (APIs) or user interfaces (UIs) for specific services. You can export a user's information from an Azure tenant via the Policy blade in the Azure portal. The steps are outlined in detail in *Azure Data Subject Requests for the GDPR*.[6]

6. Robert Mazzoli , Azure Data Subject Requests for the GDPR, Microsoft.com, June 2019. https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr-dsr-azure

05
Migrating compliance from Windows Server to Azure

Once you've reviewed the compliance (and other) benefits of migrating from Windows Server to Azure, the next step is to map out your migration plan to ensure both a smooth transition and avoidance of any compliance gaps during and after the process. Microsoft recommends a simple four-step process:

- Assess
- Migrate
- Optimize
- Manage and secure

We'll discuss each step in more detail in the following sections.

Assessment

The assessment phase begins with a "big picture" look at your on-premises resources, to identify what you have (servers and/or VMs, applications, workloads) and determine how they can be shifted to the cloud. Some will require more time and effort than others, depending on complexity and dependencies.

In addition to taking a detailed inventory, the assessment phase includes analysis and planning, using intelligent tools. You will need to collect information regarding server or VM type, configuration, usage, and applications, and then map dependencies of both servers and applications. It's also important to be aware of compatibility issues and hardware dependencies that can't be replicated in the cloud. Some workloads may need modifications to run in the cloud. Finally, you can use cost analysis tools to help determine the best IaaS VM series for your needs.

Your planning should also involve consideration of the following issues:

- **Identity management and authentication**, and how to integrate your on-premises identity solution with the cloud, preferably using a single sign-on solution.
- **Data classification**, to determine the types of data you'll be moving to the cloud and the levels of security needed for each.
- **Storage**, and which of many cloud storage options will work best for the types of data you'll be storing, and which backup and disaster recovery solutions will protect that data from loss.
- **Networking configuration** as you move from a physical to a virtual topology. You'll need to plan for how best to configure subnets and IP address ranges to make migration easier.
- **Connectivity** between your on-premises network and your virtual network in the cloud will need to support moving large amounts of data quickly.

Azure Migrate is a free, integrated service that can help you automate and expedite the assessment phase with discovery, assessment, guidance, insight, and other mechanisms for cloud migration. You can use it to migrate your physical servers as well as large-scale Hyper-V and VMware virtual machines and Azure SQL Database, as well as web applications and offline data. Azure Migrate can help you estimate the cost of your project and check for migration readiness. It also lets you take advantage of enhanced capabilities of a number of ISV tools, some of which include:

- **Azure Active Directory** can provide identity services for seamless access to cloud resources by your users.
- **Azure Storage** provides a virtual storage platform with options to meet different organizational needs, including managed storage.
- **Azure virtual networking** can support merging with your on-premises physical networking architecture to ensure that your applications can continue to use the network topology on which they were built.
- **Azure ExpressRoute** can enable a fast, private connection to Azure from your on-premises network.
- **Azure Data Box** can help migrate large amounts of data via a physical device.

Migration

After discovery, assessment, analysis, and planning are completed, the next step is selecting the migration method that's best for your organization. The approach options for each application include:

- **Rehosting** – migrating physical servers and apps to the cloud "as is," with no modification. This is the fastest and least costly method.
- **Refactoring/repackaging** – taking advantage of cloud provider services to optimize performance and reliability and reduce cost. This method requires some minor modifications to code and/or configuration.
- **Rearchitecting/redesigning** – making changes to the application's code base to optimize it for the cloud. This is time-consuming and more costly but can offer better scalability.
- **Rebuilding** – adopting PaaS or SaaS services and architecture. This can involve major revisions but can also provide new functionality.
- **Replacing** – discontinuing use of an existing application and using a SaaS solution instead. This option gets you up and running quickly with low cost up front.

The best choice for your organization depends on your goals, time constraints, budget, existing applications, and other factors. The approach you choose will determine the details of implementation. In the simplest scenario, you would create a copy of your on-premises workload in the cloud and use real-time replication to synchronize data and updates. This allows for the most seamless migration experience for your users. Once you've tested the application in the cloud and it's working correctly, you can make the switch-over and decommission the on-premises copy.

Tools you can use during the migration phase, in addition to Azure Migrate (discussed previously), include Azure Site Recovery to replicate and migrate your on-premises VMs and physical servers to Azure, Azure Database Migration Service for migrating your SQL Server databases, and third-party migration tools offered by partners.

Azure Blueprints are another tool that can help you define, set up, and update a repeatable set of Azure resources that implements and adheres to your organization's standards, patterns, and requirements. Just as architectural and engineering blueprints are used to ensure that structures comply with applicable building codes, Azure Blueprints help you deploy your migrated resources in a way that complies with your applicable regulatory requirements.

Optimization

The optimization phase is where you fine-tune your cloud deployment to realize the greatest cost savings and performance enhancement. It's also where you make any necessary adjustments to ensure that you leverage Azure compliance-related benefits.

As part of the optimization phase, you can use Azure features and services to achieve the most cost-effective and efficient environment for your workloads while maintaining or exceeding the level of compliance that you had when running your servers and applications on premises.

Some of the tools that can help you optimize your Azure VNets and VMs include:

- **Azure Cost Management**, for gaining insight into the true cost of running your systems on Azure and tracking resource usage.
- **Azure Log Analytics in Azure Monitor**, for analyzing data collected across multiple sources.

Management and security

After you've conducted a thorough assessment and mapped out a plan and then implemented it by migrating your servers and applications, and optimized your deployment to get the most out of Azure compliance, cost, and performance benefits, your job isn't over. Ongoing management and security are the key to maintaining compliance in a constantly changing regulatory environment.

The tools and techniques discussed in the Security section of this paper above will help you keep the personal data and other resources in your Azure cloud safe and private. Azure Security Center can play a key role by providing a centralized security management interface for policy management, security monitoring, remediation recommendations, and advanced defense strategies.

Azure Policy and Azure Blueprints are other tools that can help you set up and maintain ongoing compliance, as discussed in the Governance section of this paper.

06
Summary

Migrating from an on-premises Windows Server-based datacenter to a cloud computing model with Azure requires planning, but comes with benefits that make it worth the effort. These include cost savings, enhanced updatability, scalability, as well as governance and security. These latter two are especially important in an era of government and industry regulation that makes it difficult and expensive for organizations to stay in compliance without help. Azure provides that help, in the form of a secure underlying infrastructure and platform, along with tools such as Azure Migrate to make the process easier, Azure Blueprints to help ensure that the environment you deploy is compliant, and Azure security controls and encryption technologies to ensure the security and integrity of your network and the privacy of your data.

07
Further resources

Azure Compliance offerings
https://azure.microsoft.com/overview/trusted-cloud/compliance/

Azure Migrate Documentation
https://docs/microsoft.com/azure/migrate

Documentation for the Azure Blueprints service
https://docs.microsoft.com/azure/governance/blueprints/

Governance in the Microsoft Cloud Adoption Framework for Azure
https://docs.microsoft.com/azure/architecture/cloud-adoption/governance/index

An overview of Azure Blueprints (video)
https://channel9.msdn.com/Shows/Azure-Friday/An-overview-of-Azure-Blueprints

Trusted Cloud: Microsoft Azure Security, Privacy, Compliance, Reliability/Resiliency, and Intellectual Property
https://aka.ms/Azure-Trust-Paper


Microsoft