Azure Governance

An Executive View

December 2017

Microsoft

Disclaimer

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet website references, may change without notice. Customers reading this document bear the risk of using it.

This document does not provide customers with any legal rights to any intellectual property in any Microsoft product. Customers may copy and use this document for their internal, reference purposes.

The information contained in this document must not be construed as legal advice. Customers must seek their own legal counsel for advice on compliance with regulatory requirements impacting their organization

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

NOTE: Certain recommendations in this document may result in increased data, network, or compute resource usage, and may increase a customer's license or subscription costs.

Table of contents

Introduction

Microsoft Azure is a comprehensive set of cloud services to build, deploy, and manage applications through the global network of datacenters. Organization can use the Azure cloud services to efficiently build anything from simple mobile apps to internet-scale solutions. For maximum portability and value from existing investments, data and apps can flexibly connect to both the cloud and on-premises resources, since Azure offers extensive hybrid consistency.

The purpose of this document is to provide the reader with an overview on guidance that support Azure governance across risk and compliance, financial, operations, development, operations, and support. It is written to address the needs of an organization's Chief Information Officer (CIO) and other business and executive managers responsible for the evaluation, deployment, and governance of cloud services. The content of this document is divided into seven sections:

- **Section 1: Azure overview**
  This section outlines business benefits of Microsoft Azure and introduces Azure governance and the Microsoft Trusted Cloud.
- **Section 2: Risk and compliance governance**
  This section describes how Azure safeguards customer data in the cloud and provides support for organizations that are bound by regulations regarding the use, transmission, and storage of customer data.
- **Section 3: Financial governance**
  This section explains options to purchase, manage, and monitor Azure subscriptions.
- **Section 4: Development governance**
  This section describes Azure resources that can help optimize an organization’s development process and DevOps effectiveness.
- **Section 5: Operations governance**
  This section is about tools and resources to manage and monitor Azure resources, applications, and projects.
- **Section 6: Support governance**
  This section portrays a range of Azure support options for various company sizes and business needs.
- **Section 7: Governance planning**
  This section contains a summary of additional resources to help you evaluate, purchase, and manage Azure services in alignment with your business and governance objectives.

1 Azure overview

Microsoft Azure is a global cloud computing platform that features a growing collection of integrated cloud services—analytics, computing, database, mobile, networking, storage, and web. Azure includes integrated tools, prebuilt templates, and managed services that make it easier to build and manage enterprise, mobile, web, and Internet of Things (IoT) apps faster, using the skills you already have as well as the technologies you already know.

- **Deploy anywhere with your choice of tools.** Organizations are free to choose how to deploy Azure—connecting cloud and on-premises assets with consistent hybrid cloud capabilities and by using open source technologies you prefer.
    - **Build your apps, your way.** Use the tools and open source technologies you already know and trust, because Azure supports a broad selection of operating systems, programming languages, frameworks, databases, and devices.
    - **Extend on-premises data and apps.** Azure offers hybrid consistency everywhere: in application development, management and security, identity management, and across the data platform.
    - **Deploy the cloud on-premises.** Bring Azure capabilities to your datacenter with Azure Stack. Leverage the Azure portal, PowerShell, and DevOps tools experience and app model across the cloud and on-premises.

- **Protect your business with a trusted cloud.** Azure helps protect your assets through a rigorous methodology and with a focus on security, privacy, compliance, and transparency.
    - **Achieve global scale, in local regions.** Extend your global reach with the cloud service available in more countries and regions than any other provider. Azure runs on a worldwide network of Microsoft-managed datacenters across more than 36 regions.
    - **Availability Zones.** Availability Zones in Azure help to protect you from datacenter-level failures. They are located inside an Azure region, and each one has its own independent power source, network, and cooling. To ensure resiliency, there's a minimum of three separate zones in all enabled regions. The physical and logical separation of Availability Zones within a region protects an organization's applications and data from zone-level failures.
    - **Detect and mitigate threats.** Get a central view of all your Azure resources. Azure Security Center helps you prevent, detect, and respond to threats with increased visibility and control over the security of all your Azure resources.
    - **Rely on a trusted cloud.** Trust the cloud that offers comprehensive compliance coverage with more than 70 compliance certifications and attestations to comply with national, regional, and industry-specific requirements governing for example the collection and use of individuals' data.

- **Accelerate app innovation.** Build simple to complex projects within a consistent portal experience using deeply integrated cloud services, so you can rapidly develop, deploy, and manage your apps.
    - **Build apps quickly and easily**. Whether you're building internet-scale applications or simple mobile apps, develop and iterate faster and easier using the integrated tools, APIs, and analytics in Azure.
    - **Manage apps proactively.** Use the Azure portal, Application Insights, and Operations Management Suite to gain insights that help you quickly monitor, iterate, and manage your apps and systems.
    - **Deliver mobile apps seamlessly.** Build mobile apps faster for any popular form factor and operating system using continuous development and DevOps tools such as Xamarin.

For additional information on the features and benefits of Azure, please visit the Azure homepage.

1.1 Azure governance

The characteristics of the public cloud – agility, flexibility, and flexible pricing – are important to business groups that need to quickly meet the demands of customers (both internal and external). However, enterprise IT needs to ensure that data and systems are effectively protected. For this reason, business leaders must address the need for governance early and balance it with the need for agility.

Knowing where to begin can often be difficult. After deciding to use Azure, questions commonly arise, such as:

- How do I meet our legal requirements for data sovereignty in certain countries?
- How do I verify that my critical systems are not changed?
- How do I know what every resource is supporting so I can account for it and bill it back accurately?

This paper provides a starting point to address these and other issues related to Azure governance. It provides an overview of the controls, services, and guidance provided by Microsoft to support the planning, architecture, acquisition, deployment, operation, and management of an Azure subscription.

1.2 The Microsoft Trusted Cloud

Microsoft understands that for you, our enterprise customer, to realize the benefits of the cloud, you must be willing to entrust your cloud provider with one of your most valuable assets—your data. If you invest in a cloud service, you must be able to trust that your customer and employee data is safe, that the privacy of your data is protected, and that you retain ownership of and

control over your data—that it will only be used in a way that is consistent with your expectations.

To ensure we deliver technology that our customers can trust, Microsoft has established the Trusted Cloud initiative—a set of guidelines, requirements, and processes for delivering rigorous levels of engineering, legal, and compliance support. The Trusted Cloud initiative supports all our enterprise cloud services, including Microsoft Azure, Dynamics 365, and Office 365.

To find out more, please visit the Microsoft Trusted Cloud web page.

2 Risk and compliance governance

We know some organizations are still wary of the cloud because of concerns about keeping their data confidential. Microsoft understands that confidentiality is essential for any organization, which is why we have made an industry-leading commitment to the protection and privacy of your data.

Microsoft Azure has a significant number of U.S. and international certifications and attestations that demonstrate our understanding and addressing of risk and compliance issues. For example, Azure was the first cloud provider recognized by the European Union's data protection authorities for our commitment to strict EU privacy laws. The EU Model Clauses are standardized contractual clauses used in agreements between service providers (such as Microsoft) and their customers to ensure that any personal data leaving the EU will be transferred in compliance with EU data-protection law. Microsoft was also the first major cloud provider to adopt the international cloud privacy standard ISO/IEC 27018:2014.

Azure safeguards customer data in the cloud and provides support for organizations that are bound by extensive regulations regarding the use, transmission, and storage of customer data.

2.1 Compliance

Microsoft is committed to the highest levels of trust, transparency, standards conformance, and regulatory compliance. Our broad suite of cloud products and services are all built from the ground up to help address the most rigorous security and privacy demands of our customers.

- **Comprehensive compliance offerings.** To help organizations comply with international, national, regional, and industry-specific requirements governing the collection and use of individuals' data, Azure meets a comprehensive set of compliance certifications and attestations. Review all Azure compliance offerings.

- **A broad compliance framework.** Microsoft provides you with comprehensive compliance information on the Trust Center web site. This help the legal and compliance community to:
    - Understand the requirements and implications of standards conformance and regulatory compliance for cloud computing workloads
    - Articulate the value of compliance, how to use it as a competitive advantage and make more informed purchase decisions
    - Learn how Microsoft protects customers by requiring that all government requests for data access strictly respect proper legal procedures and due process

2.2 Privacy

Microsoft is a leader in creating robust cloud solutions that are designed to protect customer privacy from the ground. Our approach to privacy and data protection is rooted in our commitment to organizations' ownership of and control over the collection, use, and distribution of their data.

Microsoft understands that when you, our customer, use our business cloud services, you are entrusting us with your most valuable asset—your data. You trust that its privacy will be protected and that it will be used only in a way that is consistent with your expectations. Let us show you how.

2.2.1 Customer data

Microsoft's time-tested and proven approach to data privacy is grounded in our commitment to give you control over the collection, use, and distribution of your customer data. We are transparent about the specific policies, operational practices, and technologies that help ensure the privacy of your data in Microsoft business cloud services.

- How we manage your data. We use your customer data only to provide the services we have agreed upon, and do not mine it for marketing or advertising purposes. If you discontinue using the service, Microsoft follows strict standards and specific processes for removing your data from our systems.
- Where your data is located. Customers who must maintain their data in a specific geographic location can rely on our expanding network of datacenters around the world. Microsoft also complies with international and national data protection laws regarding transfers of customer data across borders.
- You know who can access your data and on what terms. We take strong measures to protect your data from inappropriate access, including limits for Microsoft personnel and subcontractors. Of course, you can access your own customer data at any time and for any reason.
- How we respond to government requests**.** When governments or law enforcement make a lawful request for customer data from Microsoft, we are committed to transparency and limit what we disclose. In this context it is also important that in July 2016 the Court of Appeals for the Second Circuit agreed with Microsoft that U.S. federal or state law enforcement cannot use traditional search warrants to seize emails of citizens of foreign countries that are located in data centers outside the United States.
- Stringent privacy standards. Strong contractual commitments back our privacy standards and best practices. Microsoft was the first public cloud service provider that achieved compliance with ISO/IEC 27018:2014, the first international code of practice for cloud privacy. In general, Microsoft Azure, Azure Government, and Azure Germany are audited for compliance with ISO/IEC 27001:2013 and ISO/IEC 27018:2014 at least once a year by an

accredited third-party certification body, providing independent validation that applicable security controls are in place and operating effectively.

2.2.2 General Data Protection Regulation (GDPR)

Another important topic for the privacy of customer and employee data is the General Data Protection Regulation (GDPR), which is set to take effect on 25 May 2018. The GDPR imposes new rules on companies, government agencies, non-profits, and other organizations that offer goods and services to individuals in the European Union (EU), or that collect and analyze data tied to EU residents. The GDPR applies no matter where an organization is located and where personal data is processed or stored.

Microsoft has extensive expertise not only in protecting personal data and championing privacy, but also with complying with complex regulations and helping our customers to successfully master their compliance requirements. While we are complying with EU-U.S. Privacy Shield and EU Model Clauses for quite some time already, we believe that the GDPR is an important step forward for clarifying and enabling individual data privacy rights.

Therefore, the goals of the GDPR are consistent with longstanding Microsoft commitments to security, privacy, transparency, and compliance. We are committed to GDPR compliance across our cloud services, such as Azure, when enforcement begins May 25, 2018, and provide GDPR related assurances in our contractual commitments.

In addition to that we prepared comprehensive guidance to help enterprise customers with their GDPR compliance.

- The web page Azure helps enable data privacy for GDPR compliance list provide you with a starting point to get what you need.
- We created a dedicated white paper for you to show you how Microsoft Azure can support you in your preparation for GDPR.
- The comprehensive white paper GDPR How-to: Get organized and implement the right processes contains useful information about what you can put in place to successfully address the GDPR compliance efforts of your organization.
- The Microsoft Trust Center allows you to view compliance by service, location, or industry, or by the certifications and attestations Microsoft has achieved for its cloud services. Microsoft also leads the industry in engagements with customers, regulatory bodies, and standards boards.
- Additional details about the GDPR in general and what organizations can also do as preparation for it can be found in two additional Microsoft GDPR white papers about beginning your General Data Protection Regulation journey and an overview of the (GDPR).

To find out even more, please visit the Microsoft GDPR web page.

2.3 Security

Microsoft has decades-long experience building enterprise software and running some of the largest online services in the world. We use this experience to implement and continuously improve security-aware software development, operational management, and threat-mitigation practices that are essential to the strong protection of services and data.

The guiding principle of our security strategy is to "assume breach." The Microsoft global incident response team works around the clock to mitigate the effects of any attack against our cloud services. And security is built into Microsoft business products and cloud services from the ground up, starting with the Security Development Lifecycle (SDL), a mandatory development process that embeds security requirements into every phase of the development process.

- **Auditing and logging.** Microsoft business services and products provide you with configurable security auditing and logging options to help you identify gaps in your security policies and mechanisms, and to address those gaps to help prevent breaches. Microsoft services offer some (and in some cases, all) of the following options: centralized monitoring, logging, and analysis systems to provide continuous visibility; timely alerts; and reports to help you manage the large amount of information generated by devices and services. Microsoft Azure log data can be exported to security incident and event management (SIEM) systems for detailed analysis.
- **Cybercrime.** Microsoft has invested in multiple cybersecurity teams and related facilities to address the increasing reality of cybercrime threats to our customers and our technology ecosystem. These include the Microsoft Enterprise Cybersecurity Group – a team of world-class architects, consultants, and engineers that works with organizations to help move them to the cloud more securely, modernize their IT platforms, and avoid and mitigate breaches.
- **Design and operational security.** Microsoft cloud services and software are built on the same trustworthy technology foundation that applies to all products and services. This foundation covers identity, infrastructure, apps, and data. Microsoft has also created specialized security centers of excellence to provide intensive focus on specific security issues.
- **Encryption.** For data in transit, Azure uses industry-standard transport protocols, such as TLS/SSL, between user devices and Microsoft datacenters, and within the Azure datacenters themselves. For data at rest, Azure offers a wide range of encryption capabilities including AES-256, giving you the flexibility to choose the solution that best meets your needs. If you would like to learn more about this, please visit the Security section of the Microsoft Trust Center.
- **Threat detection and prevention**. Azure offers Microsoft Antimalware for Azure Cloud Services and Virtual Machines to help you protect against online threats. We also employ intrusion detection, distributed denial-of-service (DDoS) attack prevention, regular penetration testing, and data analytics and machine learning tools to help mitigate threats to the Azure platform.

- **Central monitoring and management.** The Azure Security Center provides you with a central view of the security status of resources in your Azure subscriptions, and provides recommendations that help prevent compromised resources. It can enable more specific policies (for example, applying policies to certain resource groups that allow the enterprise to tailor their posture to the risk they are addressing).
- **Confidential computing.** In September 2017, Microsoft announced Azure confidential computing. This cutting-edge security capabilities offer a protection that so far had been missing from public clouds: encryption of data while it is in use. This means that data can be processed in the cloud while having the assurance that it is always under the control of the customer. Data is even protected from staff that has direct access to hardware. The Azure team, along with Microsoft Research, Intel, Windows, and the Microsoft Developer Tools group, have been working on Azure confidential computing software and hardware technologies to implement these security measures.

For other security resources, including tutorials and other documentation to help you customize security options in Azure services, please visit the Microsoft Azure security and Security documentation web pages.

2.4 Resources

Microsoft has compiled a wealth of resources about security, privacy, legal, and compliance topics related to Azure cloud computing.

- **Information and support.** The Microsoft Trust Center is your premier resource for learning how we implement and support security, privacy, compliance, and transparency in all our cloud products and services. The Trust Center is an important part of the Microsoft Trusted Cloud initiative and provides support and resources for the legal and compliance community. The Trust Center site provides:
  - **In-depth information** about security, privacy, and compliance offerings, policies, features, and practices across our cloud products.
  - **Recommended resources**, a curated list of the most applicable and widely used resources for each topic.
  - **Information specific to key organizational roles**, including business managers, tenant admins or data security teams, risk assessment and privacy officers, and legal compliance teams.
  - **Direct guidance and support**. If you can't find what you're looking for, please let us know what's missing (or hard to find). Our goal is to continuously improve this site to help make your job easier.
  - **Regular updates on our efforts** to strengthen the privacy, security, and compliance protections of the Microsoft cloud, including information about progress and problems,

and concrete proposals for improvement so that your organization can move forward with confidence.

- **Compliance reports.** The Service Trust Platform (STP) is a companion to the Microsoft Trust Center, and allows you to:
  - Access audit reports across Microsoft cloud services on a single page
  - Access compliance guides to help you understand how you can use Microsoft cloud service features to manage compliance with various regulations
  - Access trust documents to help you understand how Microsoft cloud services help protect your data

- **Managing compliance.** The Compliance Manager – a web-based tool available to Microsoft cloud services customers as part of the Service Trust Platform (STP) – enables you to perform real-time risk assessment, provides actionable insights, and simplifies the compliance process when using Microsoft cloud services such as Azure. As such, the Compliance Manager helps you to feel confident that you have a systems-wide view of your data protection and compliance posture while utilizing Microsoft cloud services.

  Compliance on Microsoft cloud service is based on a "shared responsibility model." The controls managed by Microsoft are compliant with various global regulatory frameworks and standards. For these Microsoft managed controls, Compliance Manager will provide you with details, for example about their implementation. You can use this information to perform risk assessments on Microsoft cloud services. However, you must also take actions to reach compliance for the controls you manage. The Compliance Manager provides one place for you to understand and oversee both our and your responsibility of implementing and testing these controls.

  Key features of the Compliance Manager are:
  - Real-time risk assessment – an intelligent score shows your compliance posture against evolving data protection regulations (for example, the GDPR and ISO 27001:2013)
  - Actionable insights – rich insights and recommended actions to improve your data protection capabilities
  - Simplified compliance – Streamline your compliance and auditing workflow with the built-in control management and audit-ready reporting tools

3 Financial governance

A key driver for customers moving to the cloud are financial opportunities to reduce cost, increase ROI, and drive market share or be left behind. Financial governance is an important component of cloud models because it helps to ensure that financial objectives can be achieved. Azure customers are typically moving from on-premises capital-intensive expenditures (Capex) to (Opex), a model based on actual usage, and need to conduct showback vs. chargeback analysis and provide mode fidelity in estimation and billing, especially for large cloud deployments. Microsoft provides several models for customers to purchase, manage, and monitor Azure subscriptions to achieve the optimal financial objectives for their requirements.

3.1 Purchase options

Azure is currently available for purchase in 100 countries or regions around the world, and Microsoft supports billing in 24 currencies. Billing for Azure services is done on a both a per-subscription and per-seat basis. A subscription is a logical grouping of Azure services that is linked to an Azure account. A singe Azure account can contain multiple subscriptions.

3.1.1 Subscription models

Several subscription types are available and have different costs and governance requirements. An organization can begin with any of the low-cost models to evaluate the Azure platform and then move to pay-as-you-go or enterprise agreements. Each model provides capabilities that need to be evaluated by a customer to determine the correct option based on need.

- **Free account.** You can create a free Azure account, which typically gives you a credit over the course of 30 days to try any combination of resources in Azure. If you exceed your credit amount, your account will be suspended. At the end of the trial, your services will be decommissioned and will no longer work. You can upgrade this to a pay-as-you-go subscription at any time. Also, you will get free access to some of the most popular products for 12 months and to more than 25 always free products. For more details, please also have a look at the Azure Free Account FAQ.

- **MSDN subscription.** If you already have an MSDN subscription, you get a predefined amount of Azure credit each month. If you exceed the credit amount, your service will be disabled until the next month starts. You can turn off the spending limit and add a credit card to be used for the additional costs. Some of these costs are discounted for MSDN accounts.

- **BizSpark account.** The Microsoft BizSpark program provides many benefits to startups. One of those benefits is access to Microsoft software for development and test environments for a predefined set of MSDN accounts. You get an Azure credit for each of those MSDN

accounts, and you pay reduced rates for several of the Azure services, such as Virtual Machines.

- **Pay-as-you-go.** With a pay-as-you-go subscription, you pay for what you use by attaching a credit card or debit card to the account. If you are an organization, you can also be approved for invoicing.

- **Enterprise agreement.** With an enterprise agreement, you commit to using a certain amount of services in Azure over the next year, and you pay that amount ahead of time. The commitment that you make is consumed throughout the year. If you exceed the commitment amount, you can pay for the extra services you have used. Depending on the amount of the commitment, you get a discounted rate on the services in Azure.

- **Additional options.** Microsoft is continuously developing new financial models to align with customer needs so they can experience the Azure platform. Current offers can be found here.

3.1.2 Vendor models ecosystem

Microsoft also has developed a global ecosystem of technology and service partners to design, build, and manage Azure solutions that are customized for your business. Marketplace partners include certified, open-source, and community software apps, add-ons, and data to help meet Azure customers' needs. Partners deliver licensing, technology, and services that complement the Azure platform.

- **Microsoft resellers.** You can work with the same resellers that you already purchase Microsoft software from using the Open Volume License Program. If you already have purchased Azure from a reseller and have an Open license key, you can activate your Azure subscription or add more credits to it here.
- **Microsoft partners.** Find a Microsoft partner who can design and implement your Azure cloud solution. These partners have the business and technology expertise to recommend solutions that meet the unique needs of your business.

3.2 Financial tools

Microsoft has developed several Azure financial planning and operational tools that customers can use to better understand the estimated costs of onboarding workloads to Azure and provide insights into usage and billing to allow for cost management and cloud resource optimization.

- **Forecast cost with the pricing calculator.** The pricing for each service in Azure is different. Many Azure services provide Basic, Standard, and Premium tiers. Typically, each tier has several price and performance levels. By using the online Pricing Calculator, you can create

pricing estimates. The calculator includes flexibility so that cost can be estimated for a single resource or a group of resources.

- **View billing information in the Azure portal.** You can download your invoice from the Azure portal or have it sent via email. To download your daily usage, go to the Azure Account Center. Only certain roles have permission to get billing invoice and usage information, such as the Account Administrator. To learn more about getting access to billing information, see Manage access to Azure billing using roles.

- **Get billing information from billing APIs.** In addition to viewing your billing information in the portal, you can access it by using a script or program through the Azure Billing REST APIs:
  - You can use the Azure Usage API to retrieve your usage data. You can fine-tune the billing usage information by tagging related Azure resources. For example, you can tag each of the resources in a resource group with a department name or project name, and then track the costs specifically for that one tag.
  - You can use the Azure Rate Card API to list all the available resources, along with the metadata and pricing information about each of those resources.

- **Set up automatic billing alerts.** After you have deployed your application or solution on Azure, you can set up automatic email billing alerts to be notified if your spend goes above an amount you configure.

- **Control how resources usage is reported and billed.** Subscription controls can be set up for separate billing and payment. Subscriptions can be used to determine the Azure resource usage of multiple departments in an organization – for example, if an organization has IT, HR, and Marketing departments and these departments have different projects running. Based on the usage of Azure resources such as virtual machines by each department, they can be billed accordingly. In this way, you can control the finances of each department.

- **Resource tracking.** As users in your organization add resources to the subscription, it becomes increasingly important to associate resources with the appropriate department, customer, and environment. Tags enable you to not only aggregate and group resources in several ways, but to use that data for chargeback purposes. For example, if you are running multiple virtual machines (VMs) for different organizations, use the tags to group usage by cost center. You can also use tags to categorize costs by runtime environment; such as, the billing usage for VMs running in production environment.

To learn more about how to understand your Azure billing and monitor usage and costs, please visit Azure Billing documentation.

4 Development governance

Azure provides a rich set of development experiences for customers to create, manage, and monitor Azure resources, applications, and projects. These experiences include connecting cloud and on-premises environments to establish consistent hybrid cloud capabilities and using a broad selection of operating systems, programming languages, frameworks, databases, and various tools, devices, and open source technologies.

By combining Azure cloud services and Azure Stack, organizations are able to accelerate the modernization of their applications across hybrid cloud environments – while balancing flexibility, control, and governance. Developers can build applications using a consistent set of Azure services, DevOps processes and tools, and governance models, and then collaborate with operations to deploy to the location (the Azure cloud or on-premises in you local data center) that best meets your business, technical, and regulatory requirements.

Even though many of the tools and technologies that you are familiar with today can be used to develop applications in Azure, there is typically a fundamental people-and-process change required to move an organization to DevOps practices and habits. Often, these organizational changes and cultural shifts slow down cloud adoption and limit consistent governance of the development life cycle.

Microsoft has developed many resources to help with the optimization of an organization's development process and DevOps effectiveness. These resource include:

- **Azure Resource Manager.** The infrastructure for your application is typically made up of many components – maybe a virtual machine, storage account, and virtual network, or a web app, database, database server, and third-party services. You do not see these components as separate entities, instead you see them as related and interdependent parts of a single entity. You want to deploy, manage, and monitor them as a group. Azure Resource Manager enables you to work with the resources in your solution as a group. You can deploy, update, or delete all the resources for your solution in a single, coordinated operation. Also, you can use a template for deployment and also use it for different types of environments such as testing, staging, and production.

- **Azure portal.** The Azure portal is a web-based application that you can use to create, manage, and remove Azure resources and services. It includes a customizable dashboard, tooling for managing Azure resources, and an entryway into subscription settings and billing information.

- **REST APIs.** Azure is built on a set of REST APIs that support the Azure portal UI. You can also use most of these REST APIs to programmatically provision and manage your Azure resources and applications from any Internet-enabled device. For the complete set of REST API documentation, see the Azure REST SDK reference.

- **APIs.** In addition to REST APIs, many Azure services also let you programmatically manage resources from your applications by using platform-specific Azure SDKs, including SDKs for the following development platforms: .NET, Node.js, Java, PHP, Python, and Ruby.

- **Monitoring and diagnostics.** Performance issues in your cloud app can affect your business. With multiple interconnected components and frequent releases, degradations can happen at any time. And if you're developing an app, your users often discover issues that you didn't find in testing. You should know about these issues immediately, and have tools for diagnosing and fixing the problems. Azure has a range of tools for identifying these problems.

- **Command-line interfaces and PowerShell**. Azure provides several ways to manage your applications and services from the command line. Usually, you can perform the same tasks from the command line as in the Azure portal—such as creating and configuring virtual machines, virtual networks, web apps, and other services.
    - **Azure CLI.** The Azure command line interface lets you connect to an Azure subscription and program various tasks against Azure resources from the command line.
    - **Azure PowerShell.** Azure PowerShell provides a set of modules with cmdlets that enable you to manage Azure resources by using Windows PowerShell.

To learn more about managing development on Azure, please refer to Understanding Azure – a guide for developers.

5 Operations governance

As organizations consider and adopt cloud services, new operational models are required to ensure that delivered cloud services will meet their capability, capacity, performance, availability, and financial objectives. These new operational models, such as DevOps, typically require IT organizations to development new skills, roles, processes, technologies, and sometimes organizational changes.

Microsoft provides a robust set of operational capabilities and tools that can be used to optimize an organization's cloud operations model based on their specific Azure platform and services usage and business and service level requirements. These capabilities include:

- **Account provisioning.** Defining account hierarchy is a major step toward using and structuring Azure services within an organization. If you have an enterprise agreement, you can further subdivide the environment into departments, accounts, and finally, subscriptions. If you do not have an enterprise agreement, consider using Azure tags at the subscription level to define hierarchy.
- **Role-based access controls.** Azure Role-Based Access Control (RBAC) enables fine-grained access management for Azure. Using RBAC, you can grant only the amount of access that users need to perform their jobs. RBAC helps you to segregate duties within a team and grant only the amount of access to users that they need to perform their jobs. Instead of giving everybody unrestricted permissions in your Azure subscription or resources, you can allow only certain actions.
- **Resource management.** Azure Resource Manager provides security, auditing, and tagging features to help you manage your resources after deployment:
    - **Activity logs.** Resource Manager logs all operations that create, modify, or delete a resource. You can use the activity logs to find an error when troubleshooting or to monitor how a user in your organization modified a resource.
    - **Customized policies**. Resource Manager enables you to create customized policies for managing your resources, so that you can reduce costs and maintain consistency in your subscription. The types of policies you create can include diverse scenarios. For example, you can enforce a naming convention on resources, limit which types and instances of resources can be deployed, or limit which regions can host a type of resource. You can also require a tag value on resources to organize billing by departments.
- **Critical resource controls.** As your organization adds core services to the subscription, it becomes increasingly important to ensure that those services are available to avoid business disruption. Resource locks enable you to restrict operations on high-value resources where modifying or deleting them would have a significant impact on your applications or cloud infrastructure. You can apply locks to a subscription, resource group, or resource. Typically, you apply locks to foundational resources such as virtual networks, gateways, and storage accounts.

- **Network access controls.** Network security groups are like firewalls in that they provide rules for how a resource can "talk" over the network. They provide fine-grained control over how/if a subnet (or virtual machine) can connect to the Internet or other subnets in the same virtual network.
- **Hybrid management.** Microsoft Operations Management Suite (OMS) is a Microsoft cloud-based IT management solution that helps you manage and protect your on-premises and Azure infrastructure. Because OMS is implemented as a cloud-based service, you can have it up and running quickly – with minimal investment in infrastructure services. OMS extends its functionalities by providing management solutions, which are prepackaged sets of logic that implement a management scenario using one or more OMS services.
- **Resource monitoring and support.** Azure resource health helps you diagnose and get support when an Azure issue affects your resources. It informs you about the current and past health of your resources and helps you mitigate issues. Whereas Azure status informs you about service issues that affect a broad set of Azure customers, resource health provides a personalized dashboard of the health of your resources. Resource health shows you all the times your resources were unavailable in the past due to Azure service issues, which makes it simple for you to understand if an SLA was violated.
- **Process automation**. Microsoft Azure Automation enables the automation of the usually manual, long-running, error-prone, and frequently repeated tasks that are commonly performed in a cloud and enterprise environment. This not only saves time and increases the reliability of regular administrative tasks, but it even can be scheduled to be automatically performed at regular intervals. You can automate processes using runbooks or automate configuration management using Desired State Configuration (DSC).

For more information, please visit Azure management + monitoring services.

6 Support governance

Azure offers a range of support options, whether you are getting started or already deploying business-critical workloads on Azure.

- **Standard – for production workloads.** The Azure Standard offering is a good choice for small or mid-size companies with minimal business critical dependence on Microsoft Azure. It includes:
    - Reactive 24x7 technical support
    - Fast initial response for support issues
    - Ability to set severity of issues
- **Professional Direct – for business-critical functions.** The Azure ProDirect offering is most appropriate for mid-size to large companies with substantial business-critical utilization of Microsoft Azure. It includes:
    - Faster initial response and escalation management for high priority issues
    - Proactive monitoring of business-critical support issues
    - ProDirect Manager provides account management from a pooled set of resources
- **Premier – for cross-product support.** The Premier offering is well-suited for large or global enterprises with strategic and business-critical dependence on Microsoft products, including Azure.
    - Complete coverage for cloud, hybrid, and on-premises solutions across all Microsoft products
    - Support available onsite in addition to online
    - Technical Account Manager is assigned to account
- **Developer – for trial, testing, and development.** The Azure Developer offering is appropriate for organizations or individuals using Microsoft Azure in non-production environments or for trial and evaluation purposes.
    - Reactive technical support
    - Support for non-Microsoft technologies running on Azure
    - Lowest priced technical support option

For more details on Azure support options, please visit Azure support.

7 Governance planning

Microsoft Azure offers resources to help you with both your purchase and management of Azure services for optimal alignment to your business and governance objectives.

- **Due Diligence.** Our Cloud Services Due Diligence Checklist can help organizations exercise due diligence as they consider moving to the cloud. It provides a structure for an organization to identify their own performance, service, data management, and governance objectives and requirements. The checklist provides a framework that aligns clause-by-clause with a new international standard for cloud service agreements, ISO/IEC 19086-1:2016. This standard offers a unified set of considerations for organizations to help them make decisions about cloud adoption, as well as create a common ground for comparing cloud service offerings.
- **Deployment best practices.** Azure Advisor is a personalized cloud consultant that helps you follow best practices to optimize your Azure deployments. It analyzes your resource configuration and usage telemetry and then recommends solutions that can help you improve the cost effectiveness, performance, high availability, and security of your Azure resources.
- **Shared responsibility.** The white paper "Shared Responsibilities for Cloud Computing" helps explain the shared roles and responsibilities an organization needs to consider when selecting a cloud model, such as IaaS, PaaS, and SaaS. The document also explores the compliance requirements that have to be considered based on the selected service model.
- **Data Governance in the face of GDPR.** The white paper "Data Governance for GDPR Compliance: Principles, Processes, and Practices" describes how a data governance plan is a driving force behind documenting the basis for protecting the privacy of and lawfully processing personal data under the General Data Protection Regulation (GDPR), the new data privacy law by the European Union. As such, an effective data governance strategy forms the foundation of an organization's approach to protecting the privacy of personal data for lawful processing. It helps to define policies, roles, and responsibilities for the access, management, security, and use of personal data. This comprehensive paper addresses data governance from concept to implementation.
- **Azure governance (article).** To help you better understand the array of governance controls implemented within Microsoft Azure from both customer and Microsoft operations perspectives, the article "Governance in Azure" provides additional information on the governance features in Azure.

For more information on Azure governance and planning, please see Trust Center Resources.

Conclusion

Microsoft Azure provides services, tools, and support to support a wide range of governance polices. Microsoft continues to build and evolve this support by business size, industry, geography and other factors to address an ever-changing governance landscape.

To keep up-to-date on the latest Azure developments supporting your governance planning, we encourage you to regularly consult the following:

- Microsoft Trust Center for in-depth information and support about security, privacy, and compliance offerings, policies, features, and practices across our cloud products, including Azure.
- Azure resources for Azure training and certification programs as well as product updates, roadmaps, webinars, events, and more.

