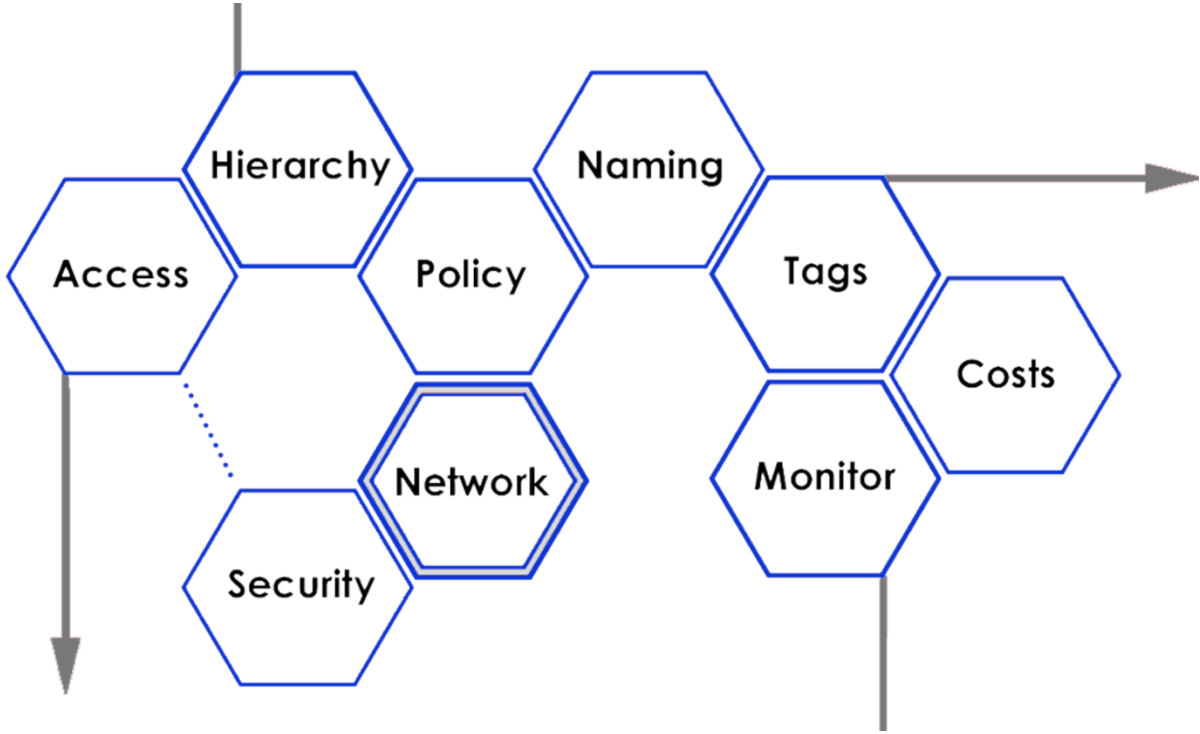


Service description document: Azure SPARK – Cloud adoption strategy

Successful cloud adoption starts with Azure Spark

Azure Spark provides a framework to assess and remedy all technical, design, security, and governance challenges raised by cloud adoption, while providing full control and financial oversight.

The framework has been developed for us to guide and support organisations to develop a cloud adoption strategy that ensures a right first-time deployment.



Some of the key benefits of this service include:

- Clarity surrounding your Azure deployment, controls and financial oversight
- Optimisation of cost measures by adopting a subscription-based model that is scaled exactly to your requirements
- Azure architecture that is tailored to your requirements
- Enhanced cloud compliance, governance and security

To develop a bespoke adoption strategy for your organisation we will provide clarity on the key deliverables required to execute your Azure adoption successfully. To achieve this, our Azure SPARK framework includes the following key deliverables:

- Management hierarchy
- Access control
- Azure policy
- Resource tagging
- Network
- Security
- Monitoring
- Cost Management

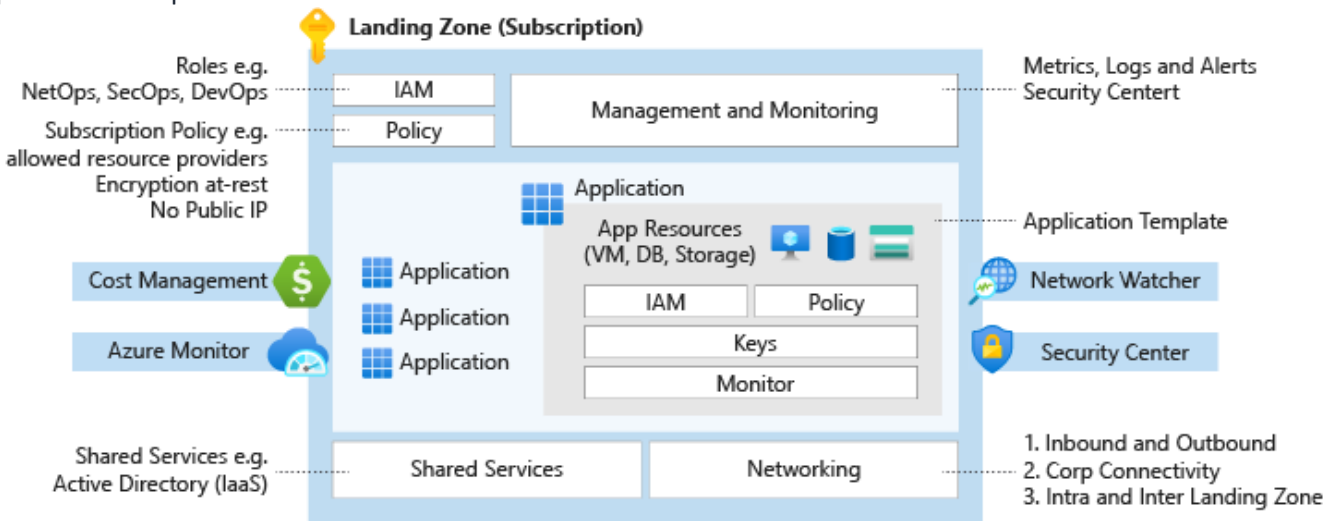
Your bespoke adoption framework

Each of the above listed key framework deliverables will be workshopped in detail with your organisations representatives and will be used to create a Cloud Adoption Framework-aligned design guideline. This will be customised based on your specific requirements.

Your existing footprint will then be assessed relative to the updated design guidelines. Where possible, the footprint will be updated. Where not, elements of the footprint can be parked as point-in-time. The exact nature of what is possible cannot be called out in this document and must be achieved via workshop and discovery.

The new design guidelines will detail a best in-class footprint (Landing Zone) suitable for both existing and future workloads. However, while it must consider the existing footprint, it will not be led by it.

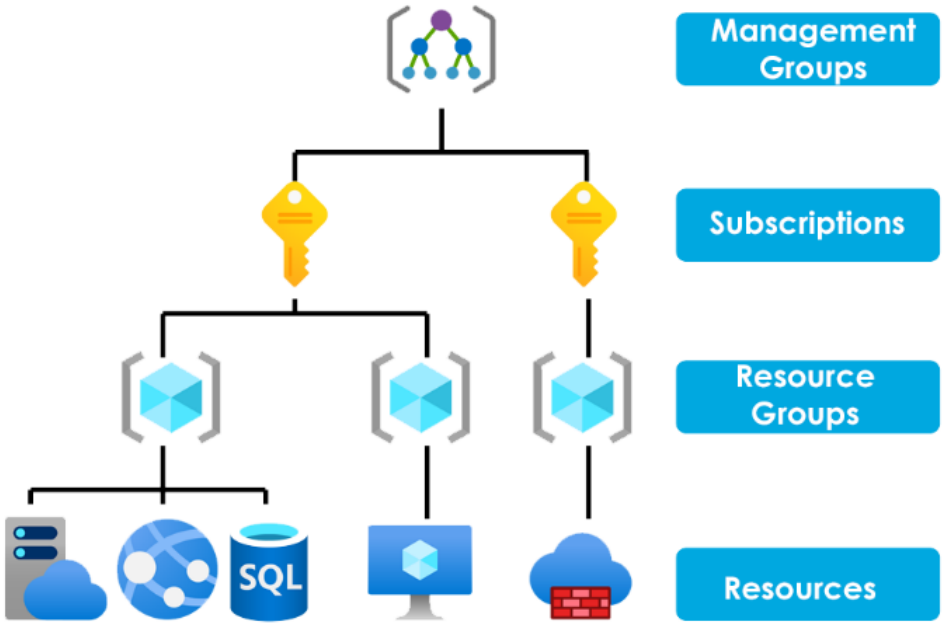
Any changes to the existing footprint outside of management pane operations will be deemed out of scope for this work but can be assessed as an effort vs reward change request. Visually, here is an example of what a component subscription of this footprint may look:



Management hierarchy

To develop your foundational Azure hierarchy design, we will work with you to develop an organisational structure for deployment and operation including:

- Regions
- Management groups (these groups are containers that help you manage access, policy, and compliance for multiple subscriptions. All subscriptions in a management group automatically inherit the conditions applied to the management group).
- Subscriptions (a subscription logically associates user accounts and the resources that were created by those user accounts. Each subscription has limits or quotas on the number of resources you can create and use. Organisations can use subscriptions to manage costs and the resources that are created by users, teams, or projects).
- Resource groups (a resource group is a logical container into which Azure resources like web apps, databases, and storage accounts are deployed and managed).



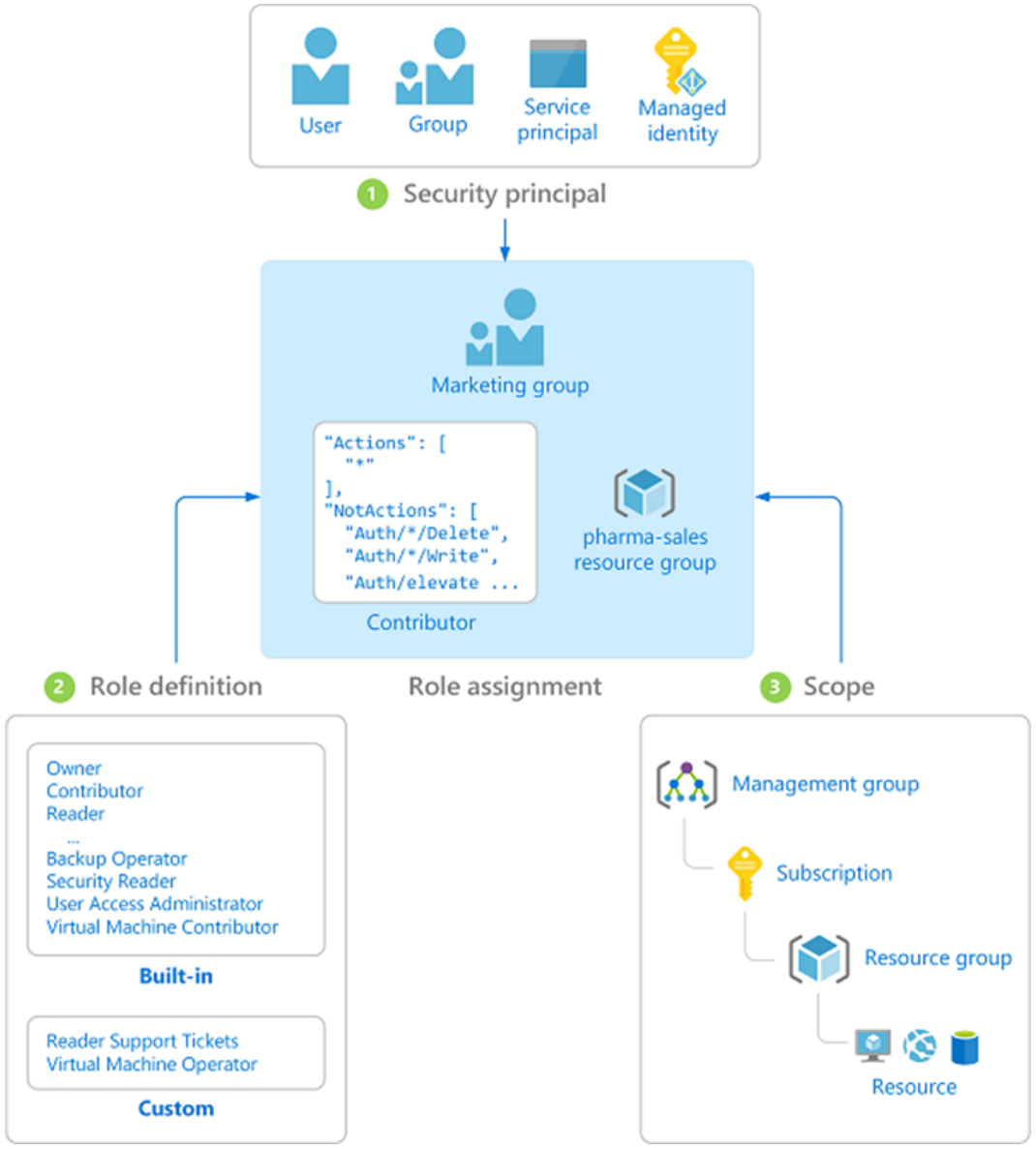
Access control

Managing who can access your Azure resources and subscriptions is an important part of your Azure governance strategy, and assigning group-based access rights and privileges is a good practice. Dealing with groups rather than individual users simplifies maintenance of access policies, provides consistent access management across teams, and reduces configuration errors. Azure role-based access control (RBAC) is the primary method of managing access in Azure.

RBAC provides detailed access management of resources in Azure. It helps you manage who has access to Azure resources, what they can do with those resources, and what scopes they can access.

When you plan your access control strategy, grant users the least privilege required to get their work done. The following image shows a suggested pattern for assigning RBAC.

eir business will work with you to design a functional, secure access policy based on your organisations requirements, in combination with recommended scope variations via role-based permissions.

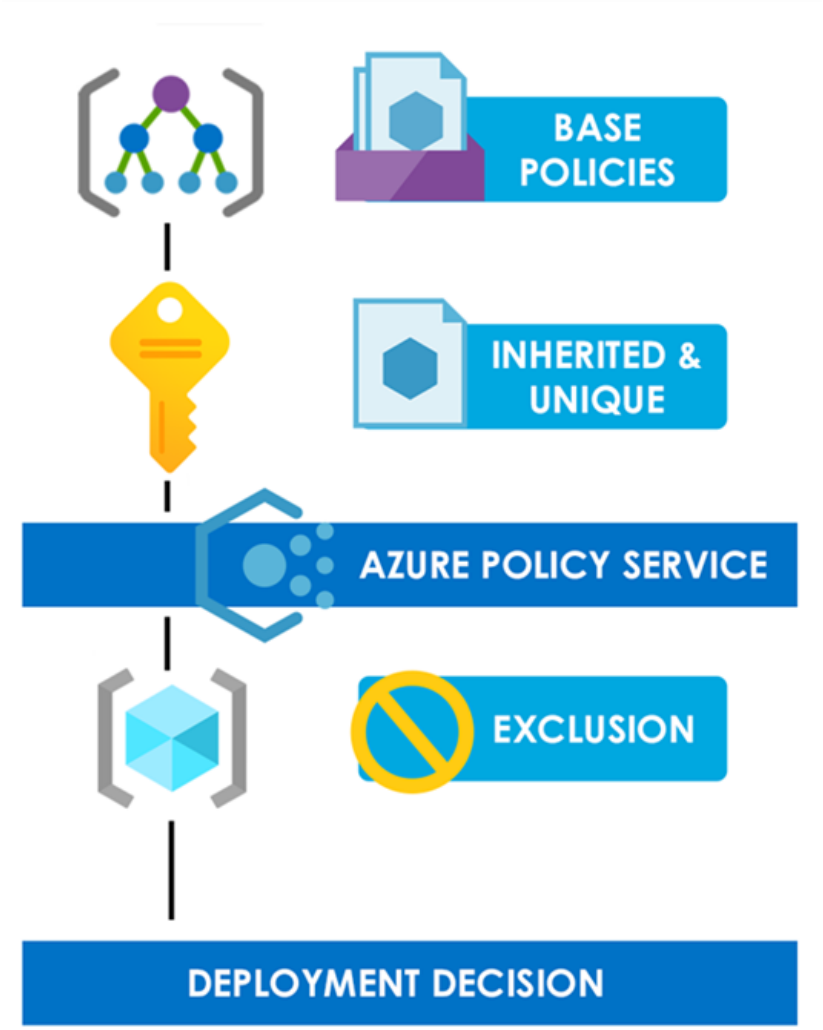


Azure policy

Azure Policy is a service that you use to create, assign, and manage policies. These policies enforce rules on your resources, so that those resources stay compliant with your corporate standards and service level agreements.

Azure Policy scans your resources to identify resources that aren't compliant with the policies you implement. For example, you can have a policy to allow only a specific virtual machine (VM) size to run in your environment.

When you implement this policy, it evaluates existing VMs in your environment and any new VMs that are deployed. The policy evaluation generates compliance events for you to use for monitoring and reporting.
Our team will work with you to shape and control the Azure platform to systematically remove, prevent, and adjust services and resources to your requirements.



Naming convention

A good naming standard helps to identify resources in the Azure portal, on a billing statement, and in automation scripts. Your naming strategy should include business and operational details as components of resource names:

- The business-related side of this strategy should ensure that resource names include the organizational information that's needed to identify the teams. Use a resource along with the business owners who are responsible for resource costs.
- The operational side should ensure that names include information that IT teams need. Use the details that identify the workload, application, environment, criticality, and other information that's useful for managing resources.

Our team will work with you to design a functional and flexible pattern-based approach to naming all resources in Azure.

Resource tagging

Tags are useful to quickly identify your resources and resource groups. You can apply tags to your Azure resources to logically organize them by categories. Each tag consists of a name and a value. For example, you can apply the name "Environment" and the value "Production" to all the resources in production. Tags should include context about the resource's associated workload or application, operational requirements, and ownership information.

After you apply tags, you can retrieve all the resources in your subscription with that tag name and value. When you organize resources for billing or management, tags can help you retrieve related resources from different resource groups. You can also use tags for many other things.

Common uses include:

- **Metadata and documentation:** Administrators can easily see detail about the resources they're working on by applying a tag like "ProjectOwner."
- **Automation:** You might have regularly running scripts that can take an action based on a tag value like "ShutdownTime" or "DeprovisionDate."
- **Cost Optimisation:** You can allocate resources to the teams and resources who are responsible for the cost. In the Azure cost management, you can apply the cost centre tag as a filter to report the charges based on a team or department usage.

Each resource or resource group can have a maximum of 50 tag name and value pairs. This limitation only applies to tags directly applied to the resource group or resource.

eir business will work with you to design a complimentary tagging policy to ensure additional useful metadata beyond name is captured.

Network

Software Defined Networking (SDN) is a network architecture designed to allow virtualized networking functionality that can be centrally managed, configured, and modified through software. SDN enables the creation of cloud-based networks using the virtualized equivalents to physical routers, firewalls, and other networking devices used in on-premises networks. SDN is critical to creating secure virtual networks on public cloud platforms such as Azure.

SDN provides several options with varying degrees of pricing and complexity. The above discovery guide provides a reference to quickly personalise these options to best align with specific business and technology strategies.

The inflection point in this guide depends on several key decisions that your cloud strategy team has made before making decisions about networking architecture. Most important among these are decisions involving your digital estate definition and subscription design (which may also require inputs from decisions made related to your cloud accounting and global markets strategies).

Small single-region deployments of fewer than 1,000 VMs are less likely to be significantly affected by this inflection point. Conversely, large adoption efforts with more than 1,000 VMs, multiple business units, or multiple geopolitical markets, could be substantially affected by your SDN decision and this key inflection point.

The hub and spoke networking model organises your Azure-based cloud network infrastructure into multiple connected virtual networks. This model allows you to manage common communication or security requirements and deal more efficiently with potential subscription limitations.

In the hub and spoke model, the *hub* is a virtual network that acts as a central location for managing external connectivity and hosting services used by multiple workloads. The *spokes* are virtual networks that host workloads and connect to the central hub through virtual network peering.

All traffic passing in or out of the workload spoke networks is routed through the hub network where it can be routed, inspected, or otherwise managed by centrally managed IT rules or processes.

This model aims to address each of the following concerns:

- **Cost savings and management efficiency.** Centralizing services that can be shared by multiple workloads, such as network virtual appliances (NVAs) and DNS servers, in a single location allows IT to minimize redundant resources and management effort across multiple workloads.
- **Overcoming subscription limits.** Large cloud-based workloads may require the use of more resources than are allowed within a single Azure subscription. Peering workload virtual networks from different subscriptions to a central hub can overcome these limits.
- **Separation of concerns.** The ability to deploy individual workloads between central IT teams and workloads teams.

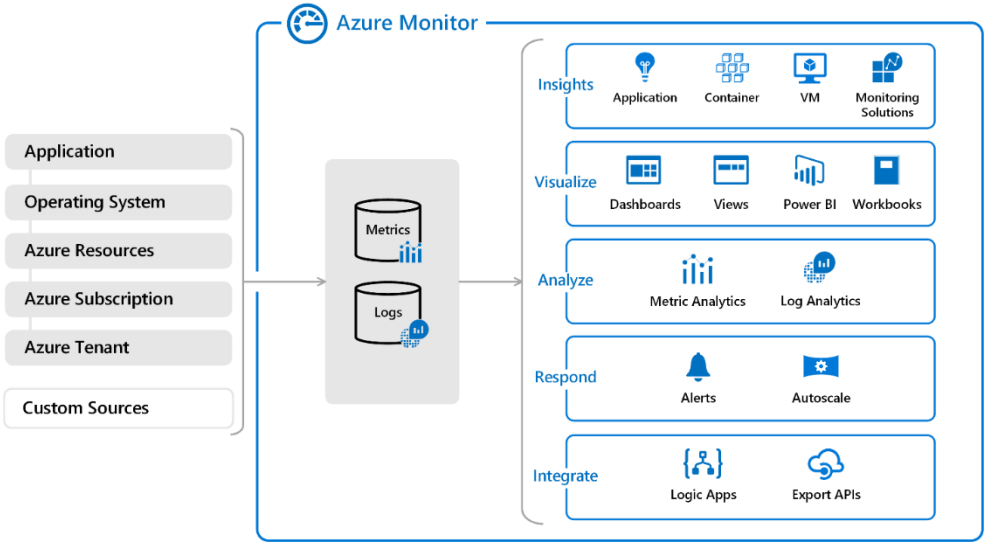
eir business will work with you to design a modern, hybrid-network footprint aligned with best practice Microsoft well architected framework guidelines.

Security

Azure security centre plays an important part in your governance strategy. It helps you stay on top of security because it:

- Provides a unified view of security across your workloads.
- Collects, searches, and analyses security data from a variety of sources, which includes firewalls and other partner solutions.
- Provides actionable security recommendations to fix issues before they can be exploited.
- Can be used to apply security policies across your hybrid cloud workloads to ensure compliance with security standards.

Many of the security features, like security policy and recommendations, are available for free. Some of the more advanced features, like just-in-time VM access and hybrid workload support, are available under the Security Centre standard tier. Just-in-time VM access can help reduce the network attack surface by controlling access to management ports on Azure VMs.



Our team will work with you to develop an agreement on platform native service adoption and systematic compliance auditing.

Monitoring

Azure Monitor provides a single unified hub for all monitoring and diagnostics data in Azure. You can use it to get visibility across your resources. With Azure Monitor, you can find and fix problems and optimise performance and:

- **Monitor and visualize metrics:** Metrics are numerical values available from Azure resources that help you understand the health of your systems. Customise charts for your dashboards and use workbooks for reporting.
- **Query and analyse logs:** Logs include activity logs and diagnostic logs from Azure. Collect additional logs from other monitoring and management solutions for your cloud or on-premises resources. Log Analytics provides a central repository to aggregate all this data. From there, you can run queries to help troubleshoot issues or to visualise data.
- **Set up alerts and actions**: Alerts proactively notify you of critical conditions. Corrective actions can be taken based on triggers from metrics, logs, or service health issues. You can set up different notifications and actions and send data to your IT service management tools.

Our team will work with you to develop an agreement of base level alert patterns and action group response details.

Azure service health

Azure Service Health provides a personalised view of the health of the Azure services and regions you use. Information about active issues is posted to Service Health to help you understand the impact to your resources. Regular updates keep you informed as the issue is resolved.

We also publish planned maintenance events to Service Health so you'll know about changes that could affect the availability of your resources. Set up Service Health alerts to be notified when service issues, planned maintenance, or other changes might affect the Azure services and regions you use.

Azure service health includes:

- Azure status: A global view of the health of Azure services.
- Service health: A personalised view of the health of your Azure services.
- Resource health: A deeper view of the health of each of your individual resources.

Cost management

Cost management is the process of effectively planning and controlling costs involved in your business. Cost management tasks are typically performed by finance, management, and app teams. Azure Cost Management can help you plan with cost in mind. It can also help you to analyse costs effectively and take action to optimise cloud spending.

Azure Cost Management provides a few ways to help you predict and manage costs:

- **Analyse cloud costs** helps you explore and analyse your costs. You can view aggregated cost for your account or view accumulated costs over time.
- **Monitor with budgets** allows you to create a budget and then configure alerts to warn you when you're close to exceeding it.
- **Optimise with recommendations** helps identify idle and underused resources so you can take action to reduce waste.
- **Manage invoices and payments** gives you visibility to your cloud investment.

Our team will work with you to develop an agreement of footprint-based budget schedules and alert patterns.


business
secure, managed solutions for all.