



OPERATIONAL ROLES AND TASKS FOR AZURE

CLOUD ROLES & RESPONSIBILITIES

Mike McKanna, PMP, ITIL
CSA-E
February 6, 2023



A man with glasses and a beard, wearing a dark suit, is looking towards a woman with long brown hair, also in business attire. They are both smiling and appear to be looking at a screen, likely a presentation or a computer monitor. The background is blurred, suggesting an office setting.

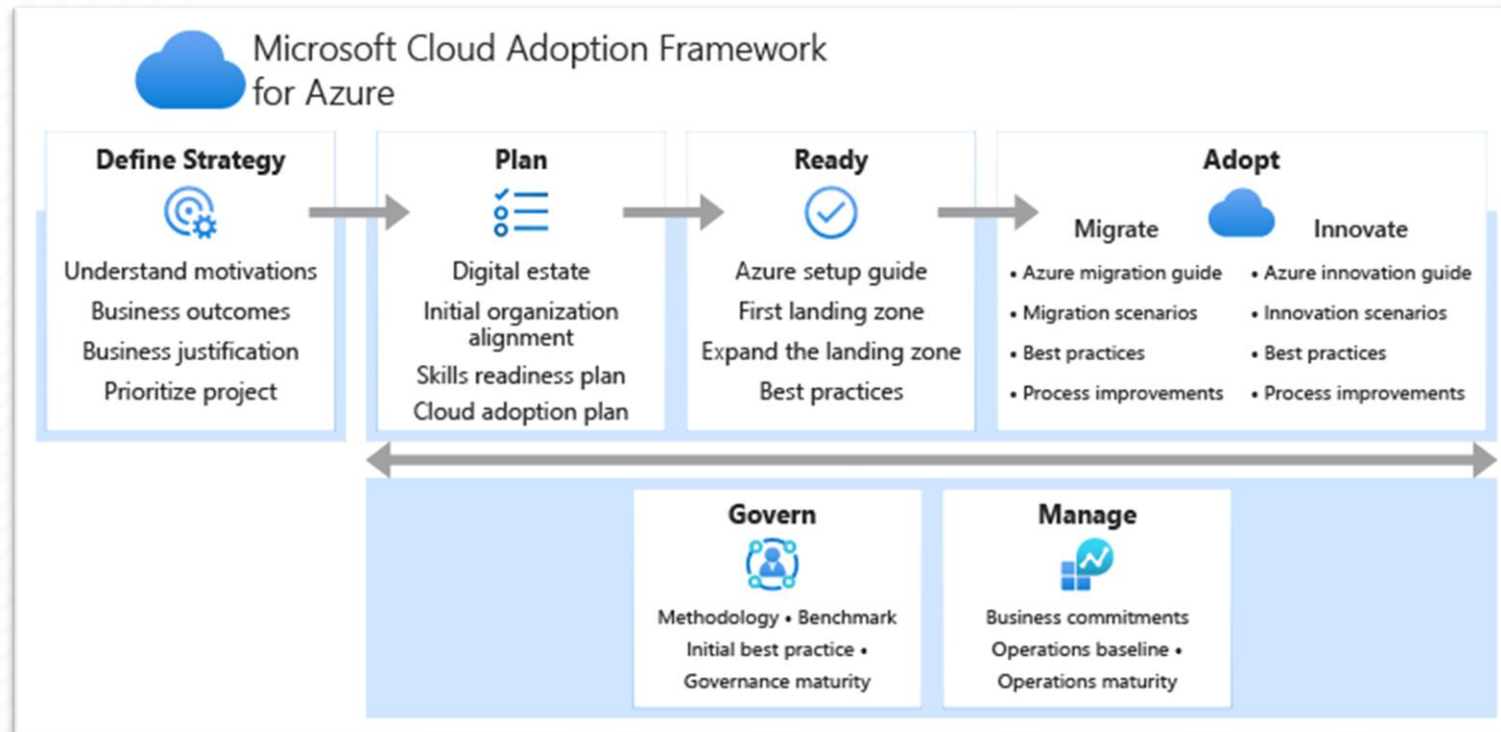
Agenda

- Cloud Adoption Framework
- Roles in The Cloud
- Cloud Operations Team
- Azure RBAC and Azure AD Roles
- Role Charts
- Cloud Operating Model

Cloud Adoption Framework

Cloud Adoption Framework

- A lifecycle approach to implement the organizational and technology strategies to succeed in the cloud
- Provides best practices, documentation, and tools

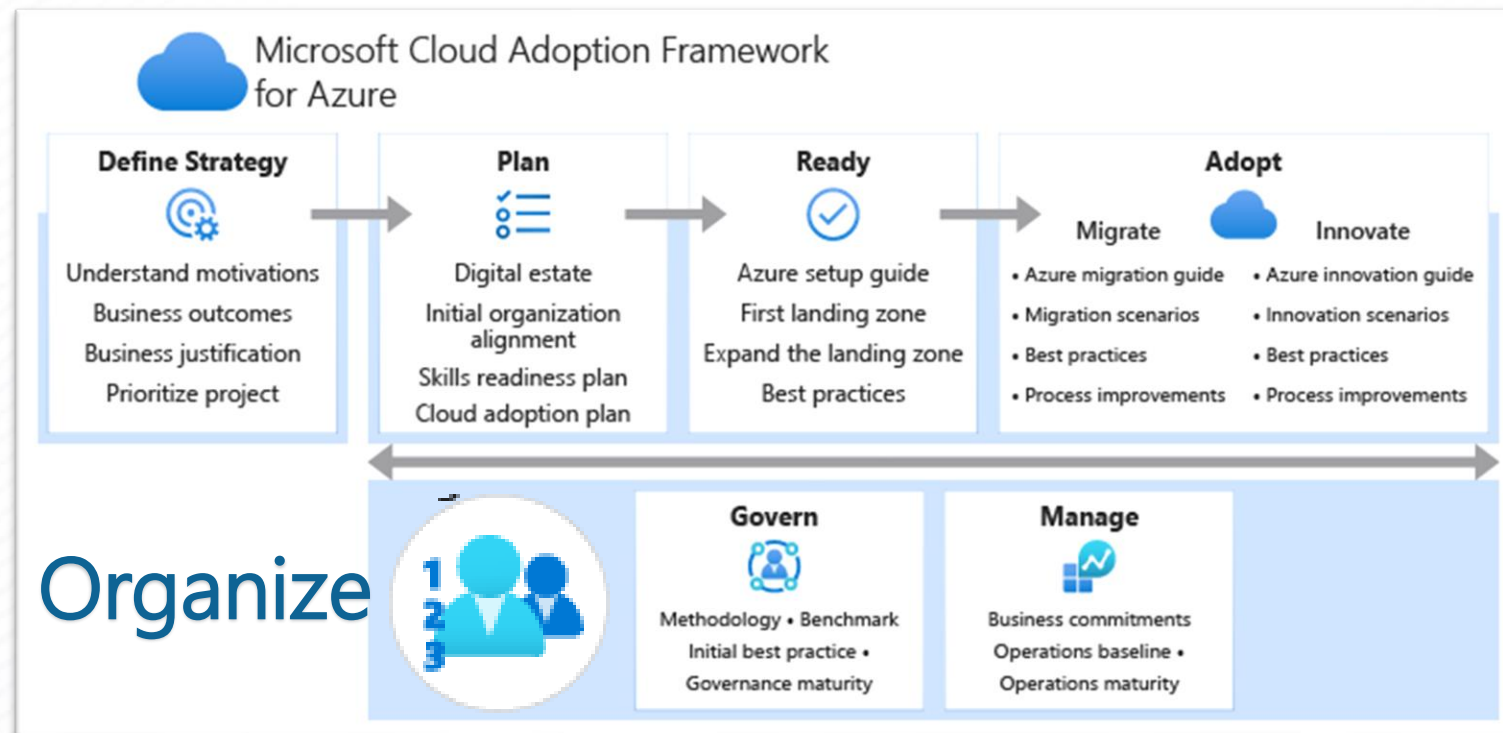


[Click the image to see the online documentation](#)



Cloud Adoption Framework

- Cloud adoption cannot happen without well-organized people
- To deliver an effective operating model for the cloud, it's important to establish appropriately staffed organizational structures



Cloud Adoption Framework Review

Understanding this critical document repository and its impact to roles & operations

Roles in the Cloud

Why We Are Here

- Cloud does not remove IT operations roles
 - BUT it **changes** them.

Some examples.



the traditional install-and-maintain paradigm becomes a deploy-and-monitor paradigm

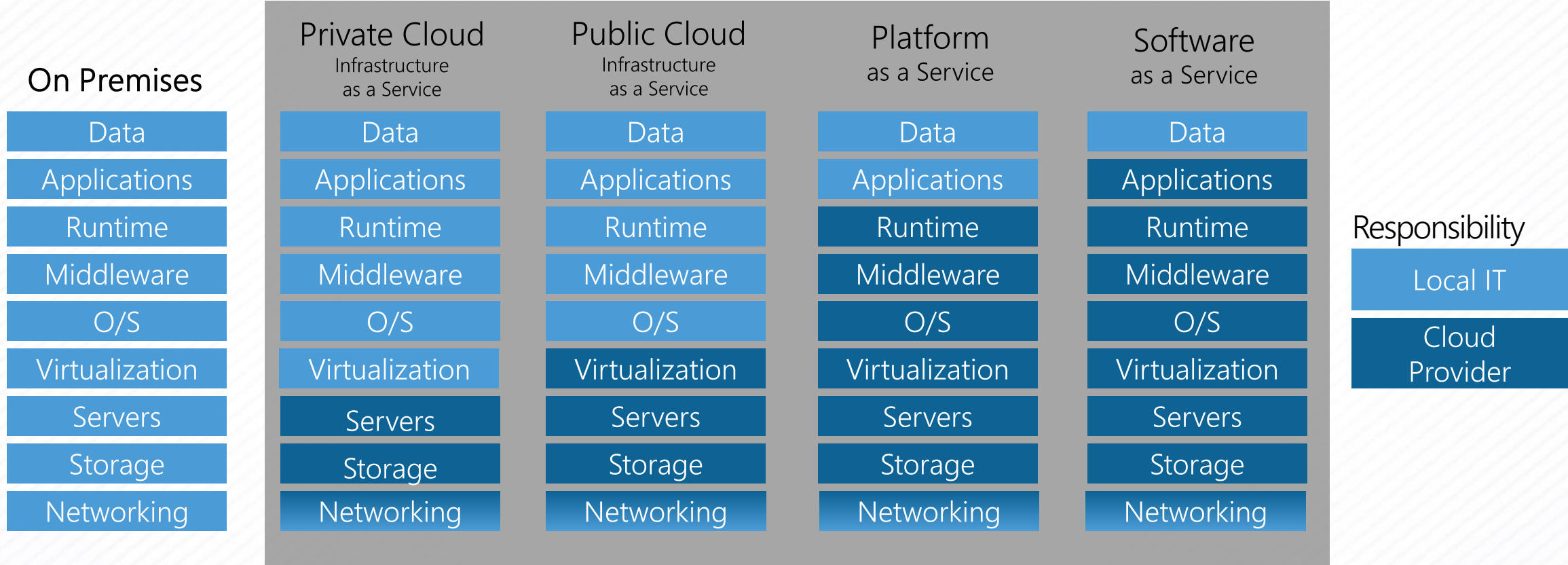


the role of IT Admin evolves in Cloud IT Admins with a reduction of the most operative tasks like *scheduled and unscheduled maintenance, updates, data recovery, storage management, monitoring.*



Cloud Operational Service is a Paradigm Shift for IT

Cloud Service Delivery Models and Shift of Operational and Support Responsibilities



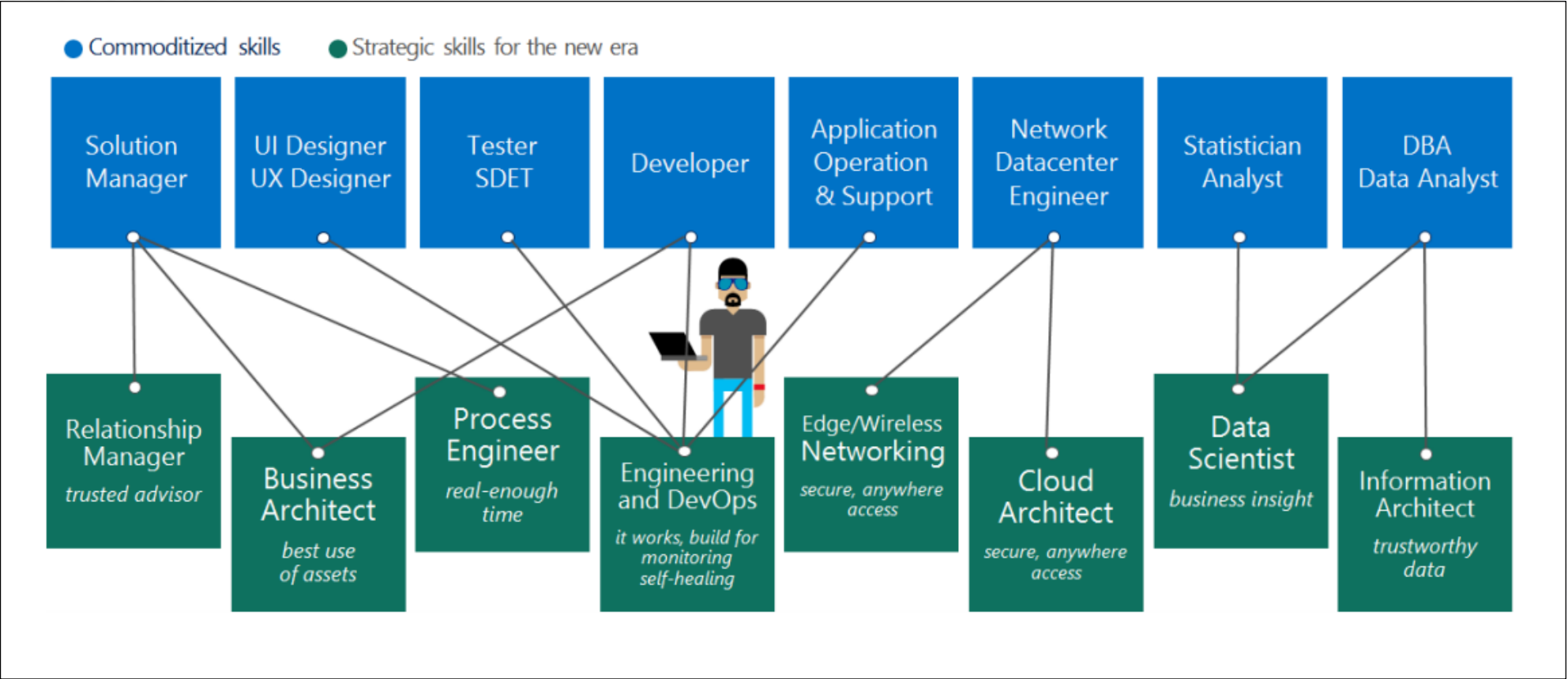

Existing staffing, structure & Operational processes


New roles and Cloud ready processes



Map Roles and Skills

Following the guidance in the Cloud Adoption Framework can aid in identifying and building the new skills required throughout the adoption lifecycle.



Click the image to see the online documentation



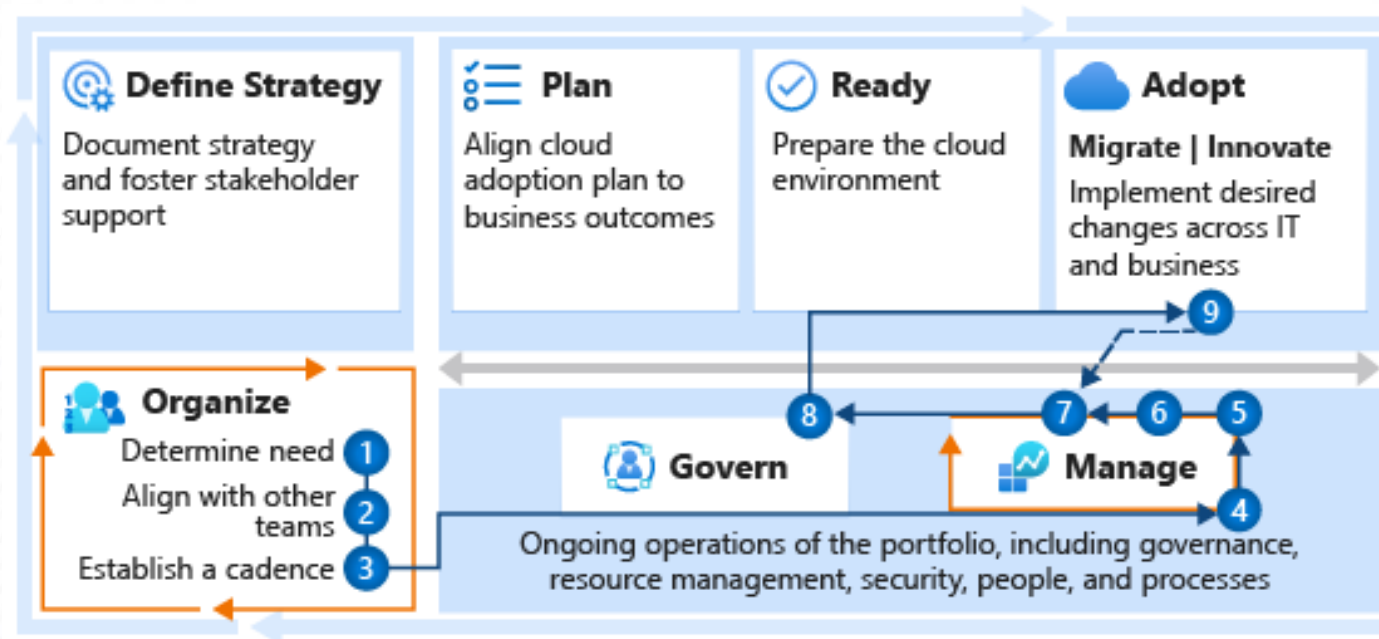
Roles in the Cloud

- As in past transitions, the most notable changes have often been marked by [changes in staff roles](#).
- Roles will likely change as organizations shift to cloud computing.
- Understanding the different available roles not only affect their ability to perform their job but also may limit their accessibility and privileges.
- Defining, understanding and assigning these roles is key in the road to roles and responsibilities:
 1. Capture concerns
 2. Identify gaps
 3. Partner across teams



Build a Cloud Operations Team

- An operations team focuses on monitoring, repairing, and remediating issues related to traditional IT operations and assets.
- In the cloud, many of the capital costs and operations activities are transferred to the cloud provider, giving IT operations the opportunity to improve and provide significant additional value.



[Click the image to see the online documentation](#)



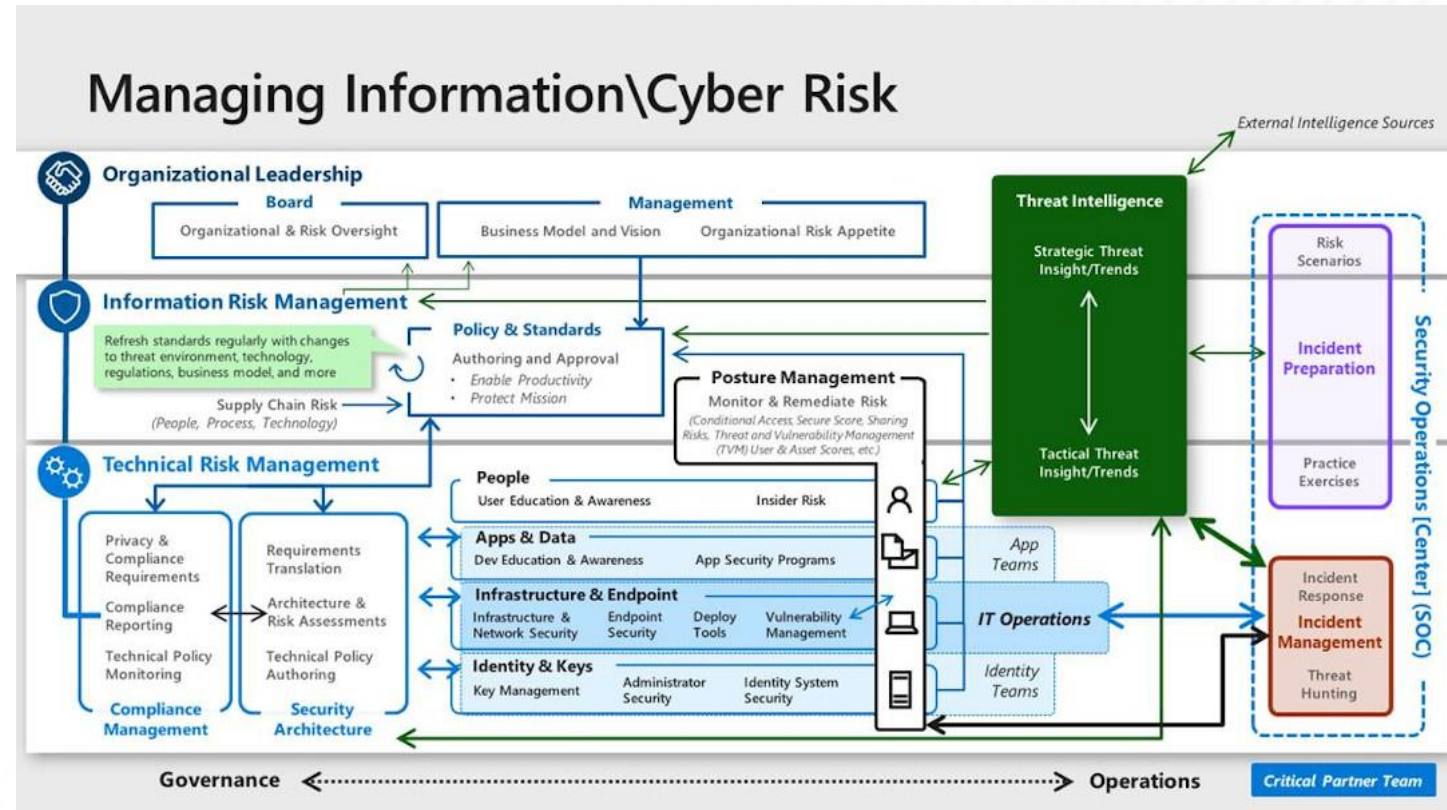
Cloud Operations Functions

- An operations team focuses on monitoring, repairing, and the remediation of issues related to traditional IT operations and assets.
- The skills needed to provide [cloud operations functions](#) can be provided by:
 - IT operations
 - Outsource IT operations vendors
 - Cloud service providers
 - Cloud-managed service providers
 - Application-specific operations teams
 - Organizational application operations teams
 - DevOps teams



Cloud Security Functions

- Security is a team sport:
 - Policy and standards
 - Security operations center (SOC)
 - Security architecture
 - Security compliance management
 - People security
 - Application security and DevSecOps
 - Data security
 - Infrastructure and endpoint security
 - Identity and keys
 - Threat intelligence
 - Posture management
 - Incident preparation

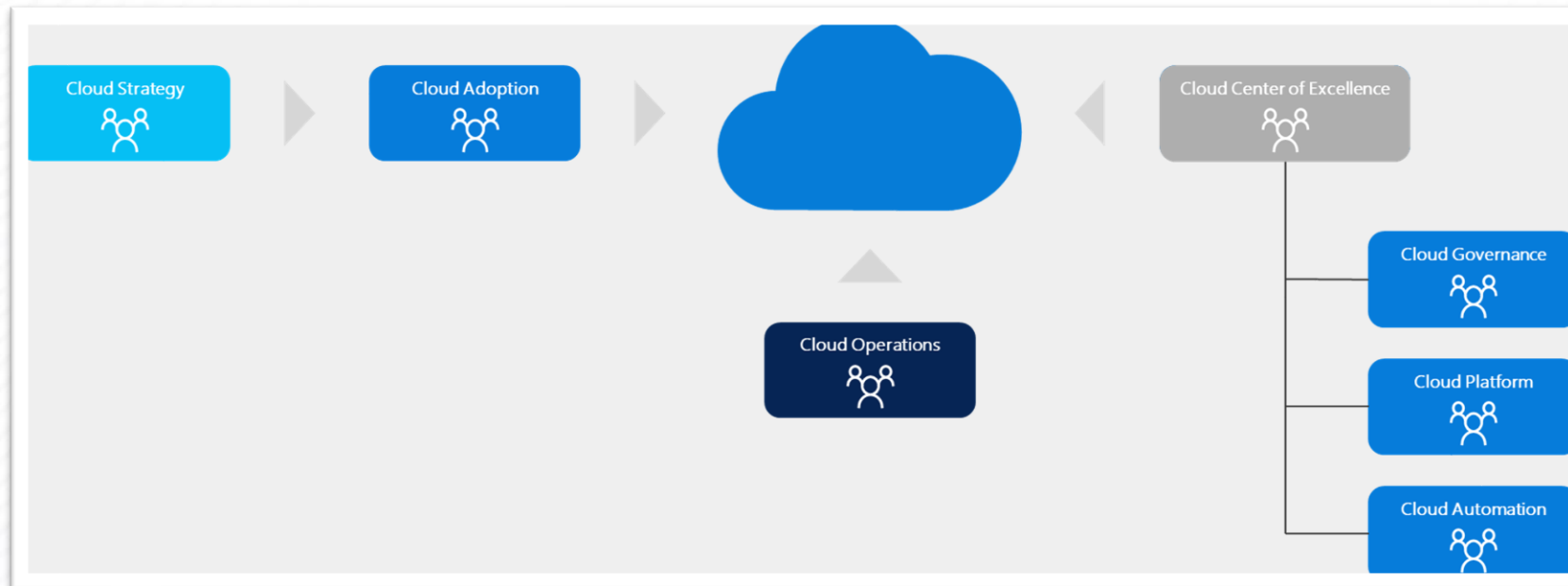


[Click the image to see the online documentation](#)



Align Your Organization

- Successful cloud adoption is the result of properly skilled people doing the appropriate types of work, in alignment with clearly defined organization goals, and in a well-managed environment.
- To deliver an effective cloud operating model, it's important to establish appropriately staffed organizational structures.

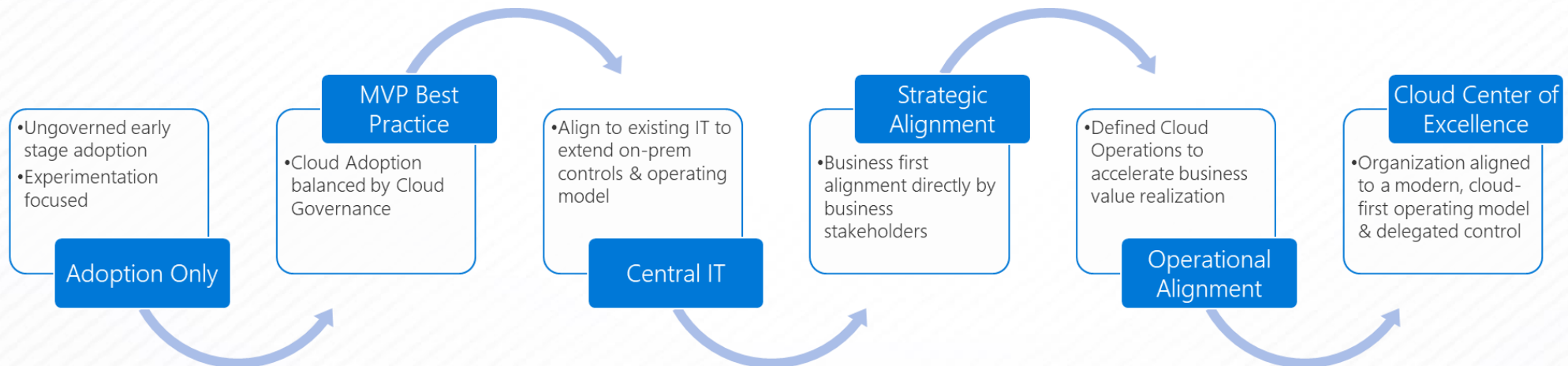


[Click the image to see the online documentation](#)



Align Responsibilities Across Teams

- Once team structures are determined, Learn to align responsibilities across teams by developing a cross-team matrix that identifies responsible, accountable, consulted, and informed (RACI) parties.
- Specify these RACI constructs:
 - The one team that is ACCOUNTABLE for a function.
 - The teams that are RESPONSIBLE for the outcomes.
 - The teams that should be CONSULTED during planning.
 - The teams that should be INFORMED when work is completed.

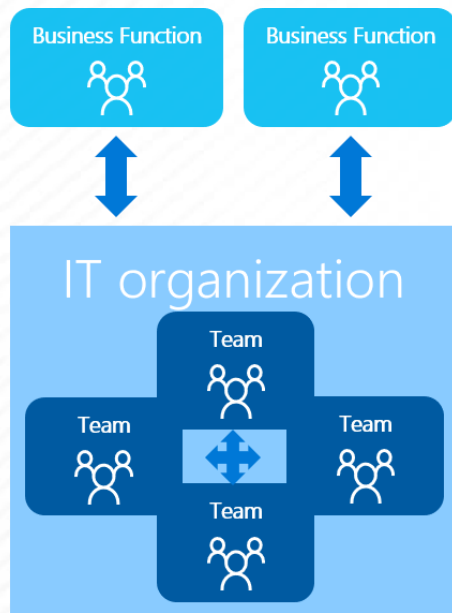


[Click the image to see the online documentation](#)

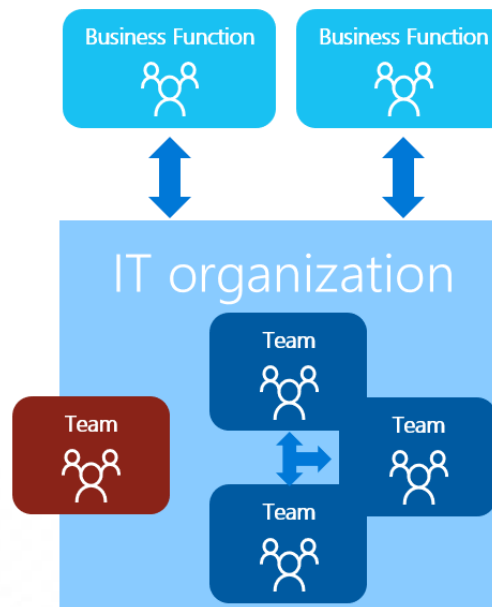


Prevent Silos and Fiefdoms

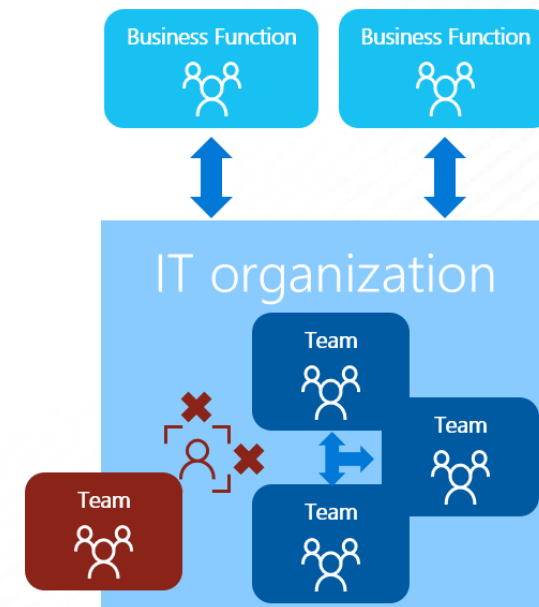
- Success in any major change to organizational practices, culture, or technology operations requires a growth mindset.
- At the heart of the growth mindset is an acceptance of change and the ability to lead despite ambiguity.



Healthy IT Team



IT Silo



Fiefdoms

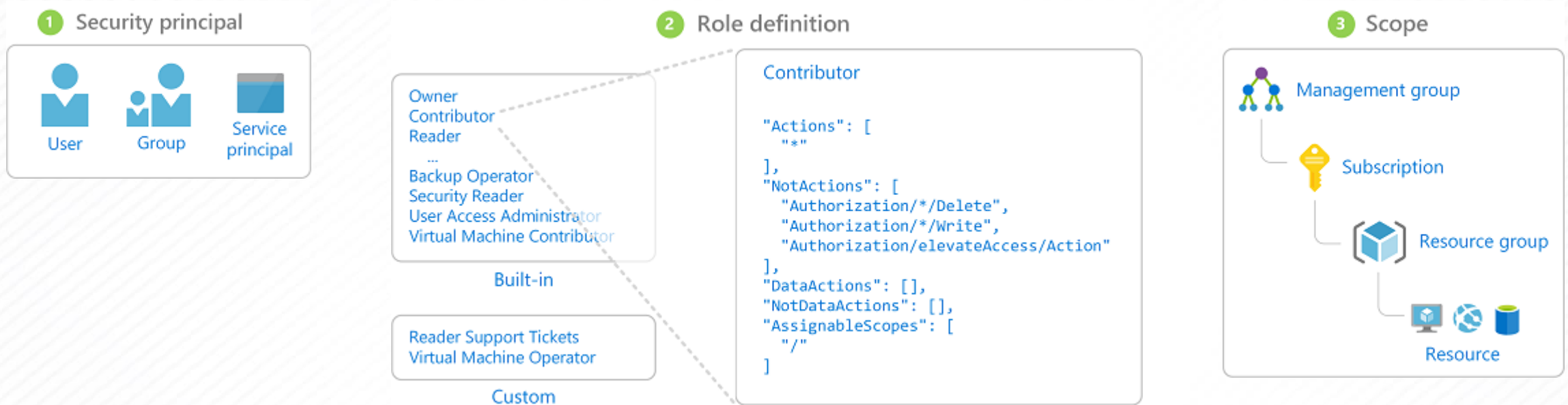
[Click the image to see the online documentation](#)



Azure Roles

Azure RBAC and Azure Active Directory

How Does Azure RBAC Work?



Security principals are assigned to a role (or many roles) and aligned to the specified scope – the boundary for which the access applies.



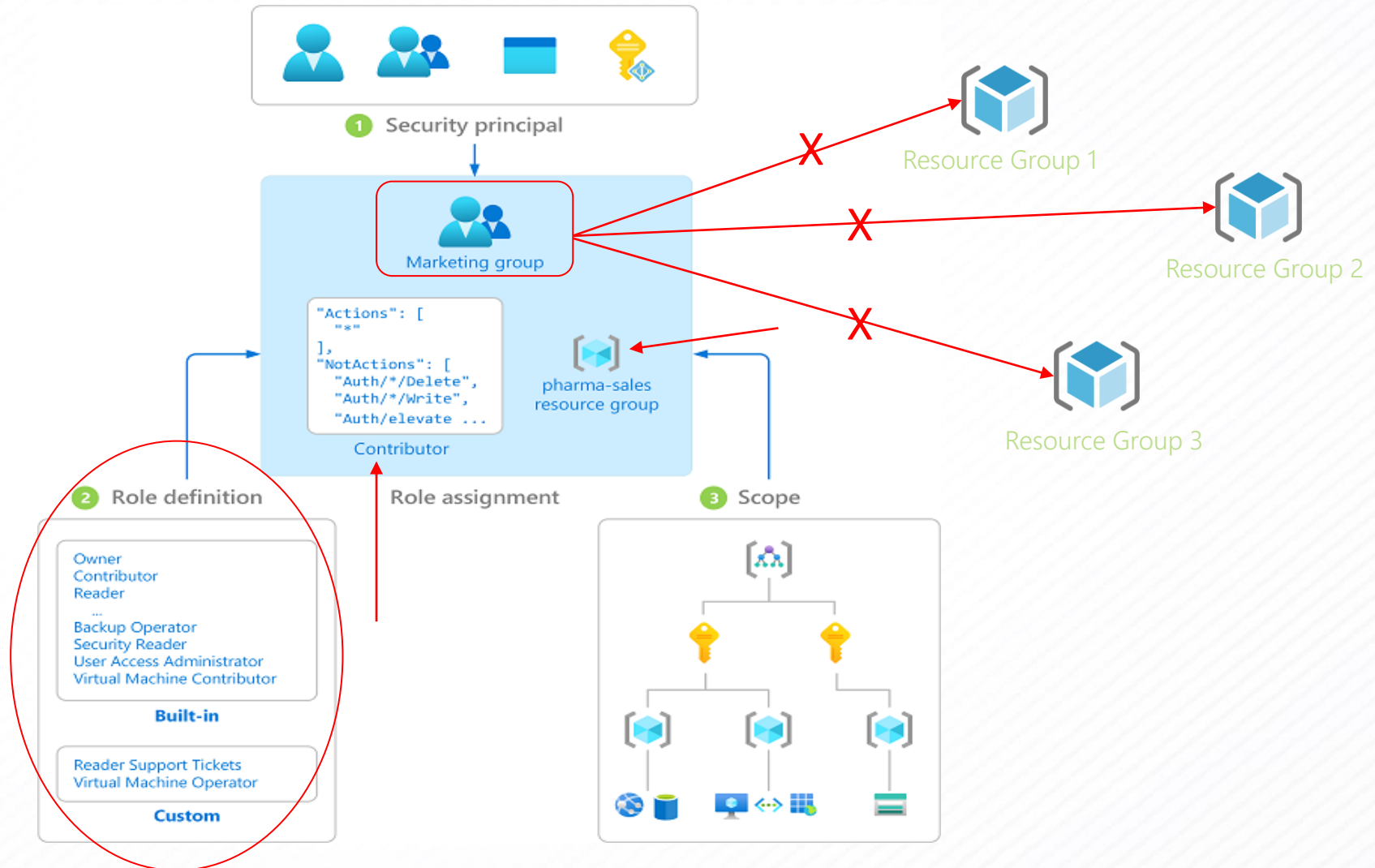
Azure RBAC Example

The Marketing group is assigned the “Contributor” role for the pharma-sales resource group.

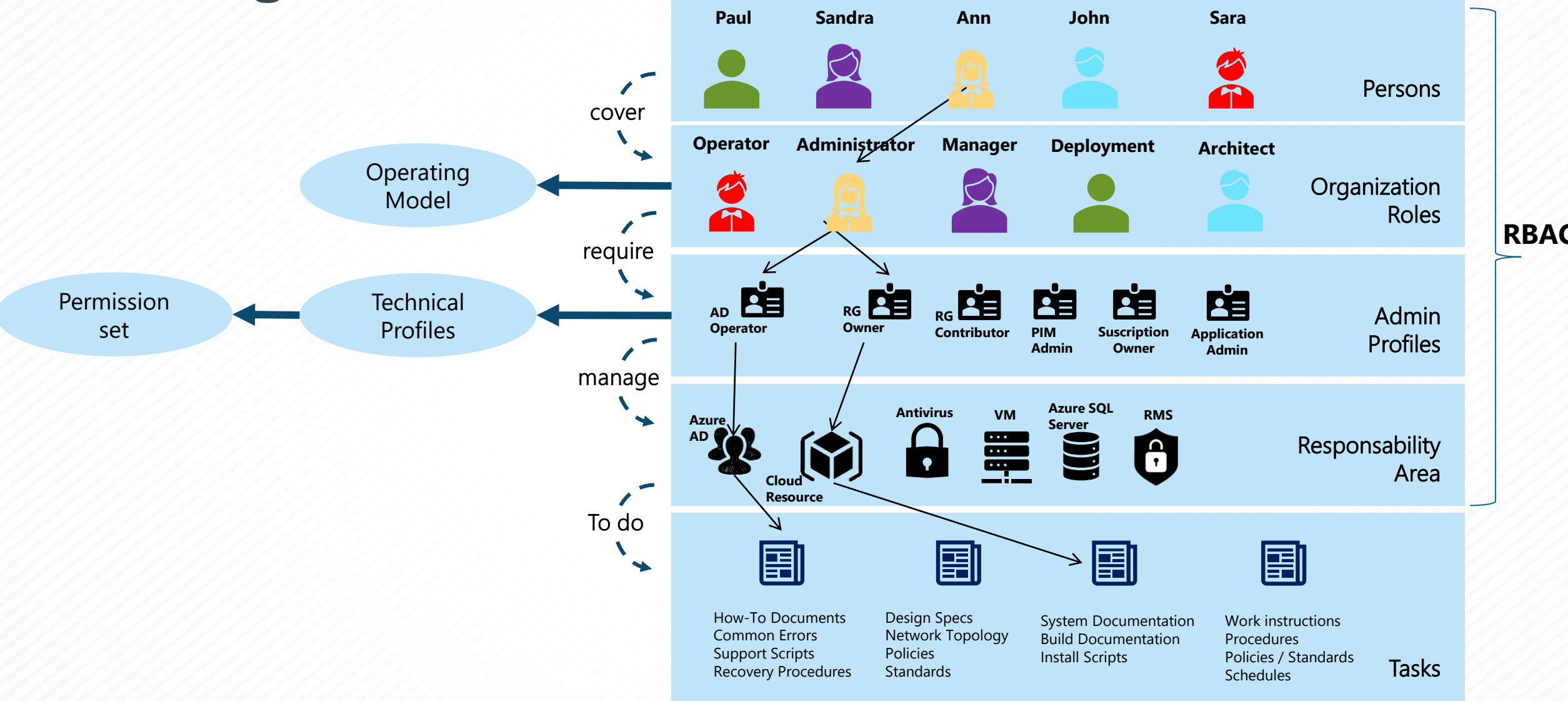
The role includes built-in RBACs plus some customs.

Now, users in the Marketing group can create or manage any Azure resource in the pharma-sales resource group.

Marketing users do not have access to resources outside the pharma-sales resource group, unless they are part of another role assignment.



Role Alignment in Azure



Example: Ann is a System administrator, with focus on a specific application on Azure.
Ann will need access to control Azure AD and manage a specific application and its dedicated RG.

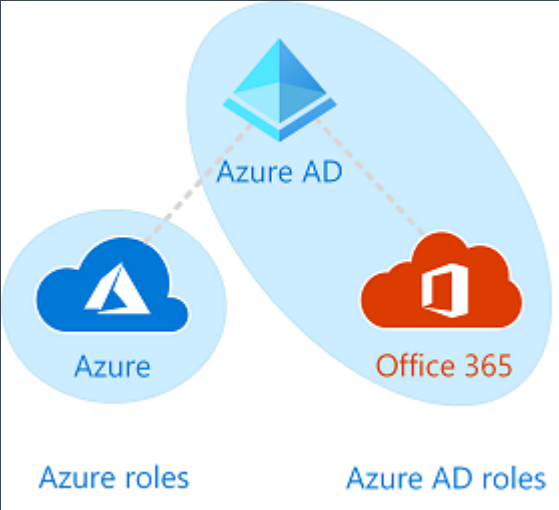


Azure Active Directory

- Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service, which helps your employees sign in and access resources:
 - External resources, such as Microsoft 365, the Azure portal, and thousands of other SaaS applications.
 - Internal resources, such as apps on your organizational network and intranet, along with any cloud apps developed by your own organization.
- An Azure subscription has a trust relationship with Azure Active Directory (Azure AD) to authenticate users, services, and devices – the relationship can only exist to one Azure AD directory.
- When a subscription expires, the trusted instance of the Azure AD service remains, but the security principals lose access to Azure resources.



Azure RBAC vs. Azure AD Admin Roles



Azure RBAC roles	Azure AD administrator roles
Manage access to Azure resources	Manage access to Azure Active Directory resources
Supports custom roles	Cannot create your own roles
Scope can be specified at multiple levels (management group, subscription, resource group, resource)	Scope is at the tenant level
Role information can be accessed in Azure portal, Azure CLI, Azure PowerShell, Azure Resource Manager templates, REST API	Role information can be accessed in Azure admin portal, Office 365 admin portal, Microsoft Graph, AzureAD PowerShell



Main Roles for Azure Administration

This administration model evolves all the time. For the most updated information it is recommended to use the online [model](#)

Subscription administration



Account
Admin



Service
Admin



Co-
Admin

Azure Resource Management



Owner



Contribu
tor



Reader



User
Access
Admin

Azure Active Directory



Global
Admin



Billing
Admin



License
Admin



Helpdesk
Admin



Service
Admin



Cloud App
Admin



Cloud
Device
Admin



Appl
Developer



Security
Admin



Azure Roles

Role Charts

Role Visual Chart



Role
Name

<div>Description<div></div></div> <div>It gives you a high-level introduction about this role.</div>		
<div>Responsibilities<div></div></div> <div>Lists main responsibility this role has.</div>	<div>Tips<div></div></div> <div>Lists some advice when you consider this role</div>	<div>Area<div></div></div> <div>Scenario where this role acts among Global, Other, Identity, and so on</div>
		<div>Scope<div></div></div> <div>Scope role among Subscription, Resource Group, Resource, etc...</div>
	<div>Process involvement<div></div></div> <div>Lists the role involvement with main IT processes</div>	<div>General comments<div></div></div> <div>General comments shares with you</div>
		<div>Operating Model<div></div></div> <div>Highlights the link with the schema we met early among Strategic, Tactical and Operational</div>



Account Administrator



Account
Admin

Description



Has full access to the Azure subscription. The account that is used to sign up for Azure is automatically set as both the Account Administrator and Service Administrator.

Responsibilities



- Manage billing in the Azure portal
- Manage all subscriptions in an account
- Create new subscriptions
- Cancel subscriptions
- Change the billing for a subscription
- Change the Service Administrator

Tips



- Must be limited to a few people in your organization.
- This role can be hosted in a team which is not part of IT (i.e. Finance, Accounting...)
- 1 per Azure account

Area



- Global

Scope



- Subscription

Process involvement



- Incident Management
- Change Management
- Monitoring
- Management of escalations to Microsoft
- Billing Management
- Service Catalog Management

General comments



- He's not a Technology administrator
- Conceptually, the billing owner of the subscription.

Operating Model



- Tactical / Technical Level



Service Administrator



Service
Admin

Description



By default, for a new subscription, the Account Administrator is also the Service Administrator, he has full access to the Azure portal.

Responsibilities



- Manage services in the Azure portal
- Cancel the subscription
- Assign users to the Co-Administrator role

Tips



- Must be limited to a few people in your organization.
- This role must be on the IT side.
- 1 per Azure subscription

Area



- Global

Scope



- Subscription

Process involvement



- Incident Management
- Change Management
- Monitoring
- Management of escalations to Microsoft
- Billing Management

General comments



- The Service Administrator has the equivalent access of a user who is assigned the Owner role at the subscription scope.

Operating Model



- Tactical / Technical Level



Co-Administrator



Co-Admin

Description



By default, for a new subscription, the Account Administrator is also the Service Administrator, he has full access to the Azure portal.

Responsibilities



- Manage services in the Azure portal
- Cancel the subscription
- Assign users to the Co-Administrator role
- He can't change the association of subscriptions to Azure directories
- Assign users to the Co-Administrator role, but cannot change the Service Administrator

Tips



- Must be limited to a few people in your organization.
- This role must be on the IT side.
- 200 per subscription

Area



- Global

Scope



- Subscription

Process involvement



- Incident Management
- Change Management
- Monitoring
- Management of escalations to Microsoft
- Billing Management

General comments



- The Co-Administrator has the equivalent access of a user who is assigned the Owner role at the subscription scope..

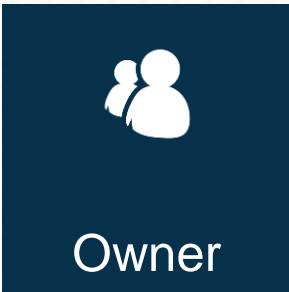
Operating Model



- Operational Level



Owner (RBAC)



Description			
Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.			
Responsibilities	Tips	Scope	
<ul style="list-style-type: none">Full access to all resourcesDelegate access to others	<ul style="list-style-type: none">The Service Administrator and Co-Administrators are assigned the Owner role at the subscription scopeCreate a custom role only if built-in RBACs don't address your need.Role can be assigned to user in every organization unit within the company.	<ul style="list-style-type: none">Root Management GroupManagement GroupSubscriptionResource GroupResource	
Process involvement		General comments	
<ul style="list-style-type: none">Incident ManagementChange ManagementOperations / ConfigurationsMonitoringManagement of escalations to MicrosoftBilling ManagementService Level Management		<ul style="list-style-type: none">Applies to all resource types.	
Operating Model		<ul style="list-style-type: none">Tactical / Technical Level	



Contributor (RBAC)



Contributor

Description



Grants full access to manage all resources but does not allow you to assign roles in Azure RBAC, manage assignments in Azure Blueprints, or share image galleries.

Responsibilities



- Create and manage all of types of Azure resources:
 - roles
 - Policy
 - Assignment
 - Policy definition
 - Policy set definition
 - Blueprint assignment
- Create a new tenant in Azure Active Directory
- Cannot grant access to others

Tips



- Create a custom role only if built-in RBACs don't address your need.
- Role can be assigned to user in every organization unit within the company.

Scope



- Root Management Group
- Management Group
- Subscription
- Resource Group
- Resource

Process involvement



- Incident Management
- Change Management
- Operations / Configurations
- Monitoring
- Management of escalations to Microsoft
- Billing Management
- Service Level Management

General comments



- Applies to all resource types.

Operating Model











- Tactical / Technical Level



Reader (RBAC)



Reader

Description 		
View all resources but does not allow you to make any changes.		
Responsibilities 	Tips 	Scope 
<ul style="list-style-type: none">View Azure resources	<ul style="list-style-type: none">Create a custom role only if built-in RBACs don't address your need.Role can be assigned to user in every organization unit within the company.	<ul style="list-style-type: none">Root Management GroupManagement GroupSubscriptionResource GroupResource
	Process involvement 	General comments 
	<ul style="list-style-type: none">Monitoring	<ul style="list-style-type: none">Applies to all resource types.
		Operating Model 
		<ul style="list-style-type: none">Tactical / Technical Level 



Security Administrator



Security
Admin

Description



Manage Customer Lockbox requests, can turn Customer Lockbox capability on or off.

Responsibilities



- Create and manage payloads in Attack simulations in the Microsoft 365 Security center
- Create and manage simulations in the Microsoft 365 Security center
- Read and configure Service Health in the Microsoft 365 admin center AND Azure portal
- Create and manage service requests in the Microsoft 365 admin center AND Azure portal
- Create, modify and delete policies
- Create , modify and delete conditional access policies
- Read all properties on audit logs, including privileged properties
- Read BitLocker keys
- Read and update all resources in Azure AD Identity Protection
- Set secondary roles where they are present

Tips



- Must be limited to a few people in your organization.
- This role can be hosted in a team which is not part of IT (i.e. Security OU).

Area



- Security & Compliance

Scope



- Security

Process involvement



- Incidents & Problem Management
- Management of escalations to Microsoft
- Operations / Configurations
- Management of escalations to Microsoft
- Monitoring (technical & usage)
- Change Management
- Knowledge Management
- L1 & L2 steering

General comments



- Control your organization's overall security
- Create and manage security policies
- Review security policies and reports
- Monitor the threat landscape

Operating Model



- Tactical / Technical Level



Security Operator



Security
Operator

Description



Investigate and response to security alerts, manages features in Identity Protection center, monitors service health.

Responsibilities



- Read and configure Service Health in the Microsoft 365 admin center AND Azure portal
- Create and manage service requests in the Microsoft 365 admin center AND Azure portal
- Create and delete all resources, and read and update standard properties in:
 - Microsoft Cloud App Security
 - Azure AD Identity Protection
 - Microsoft Defender Advanced Threat Protection
- Manage all aspects of Azure Advanced Threat Protection
- Create and delete all resources, and read and update standard properties in the Security & Compliance Center

Tips



- Must be limited to a few people in your organization.
- This role can be hosted in a team which is not part of IT (i.e. Security OU).

Area



- Security & Compliance

Scope



- Security

Process involvement



- Incidents & Problem Management
- Management of escalations to Microsoft
- Knowledge Management

General comments



- Do not reset passwords
- View security reports and policies for role assignments
- View Intune user, device, enrollment configuration, and application information

Operating Model



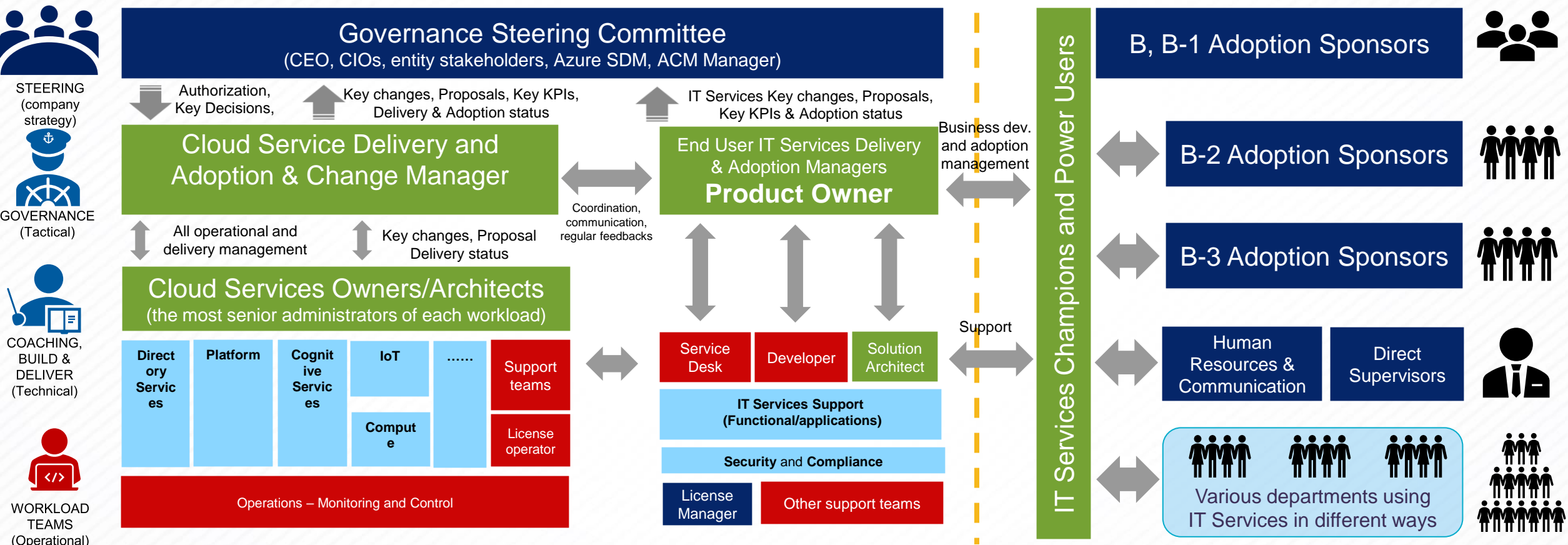
- Operational Level



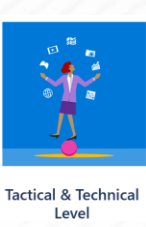
Operating Model: Cloud governance examples (Azure)

Global IT Delivery Organization

Organizational Leadership



Operating Model: Strategic Level Examples



Role	Responsibilities	Scenario (*)
Governance Steering Committee - Chairman	Who takes strategic decisions about solutions and their adoption inside own organization; it could be located both inside or outside IT Dept.	New (Cloud)
Gov / Steering Committee - Member	A Steering Committee member responsible for committee organization and agenda management/definition	New (Cloud)
Adoption Sponsor	Business sponsors . There must be one for each solution/service/product in your service portfolio	Current
License / Cost Manager	Who defines the financial strategies and target users for each solution.	New (Cloud)

(*): The **New (Cloud)** value refers to those roles introduced with cloud world, while the **Current** value refers to those roles already in place in the On-Premise scenario too.



Operating Model: Tactical Level Examples



Strategic Level



Tactical & Technical Level



Operational Level

Role	Responsibilities	Scenario (*)
Cloud Service Delivery & ACM	Who manages the cloud service itself to: * highlight the organization ROI in their adoption as usage, * and consumption plus maintaining vendor relationship .	New (Cloud)
Cloud Service Owners / Architects (Networking)	Who defines standards, policy, rules and architectures for specific workload to help organization embraces them. There must be one for the area covered Azure products as Virtual Network, Express Routes, Load Balancer, DNS, CDN, etc...	New (Cloud)
Cloud Service Owners / Architects (Storage)	Who defines standards, policy, rules and architectures for specific workload to help organization embraces them. There must be one for the area covered Azure products as Storage Account, Blob containers, Disks, Azure Backup, Azure NetApp files, etc....	New (Cloud)
Cloud Service Owners / Architects (Identity)	Who defines standards, policy, rules and architectures for specific workload to help organization embraces them. There must be one for the area covered Azure products as Azure Active Directory .	New (Cloud)
Cloud Service Owners / Architects (Compute)	Who defines standards, policy, rules and architectures for cross workloads to help organization embraces them. There must be one for the area covered Azure products as Virtual Machines, VM Scale Sets, etc...	New (Cloud)
Cloud Service Owners / Architects (Security)	Who defines standards, policy, rules and architectures for cross workloads to help organization embraces them. There must be one for the area covered Azure products as Security Center, Key Vault, Conditional Access, Azure Defender, etc...	New (Cloud)
Cloud Service Owners / Architects (Compliance)	Who defines standards, policy, rules and architectures for cross workloads to help organization embraces them. There must be one for the area covered Azure products as Azure Active Directory .	New (Cloud)

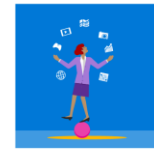
(*): The **New (Cloud)** value refers to those roles introduced with cloud world, while the **Current** value refers to those roles already in place in the On-Premise scenario too.



Operating Model: Operational Examples



Strategic Level



Tactical & Technical Level



Operational Level

Role	Responsibilities	Scenario (*)
Operations (Monitoring & Control)	Who's guaranteeing service quality as performance, availability through daily operations about cloud service.	Current
Developers (DevOps)	Daily operations about each application.	New (Cloud)
Operators (Platform)	Who manages the Identity Management tasks or Azure Portal and their control in respect of policy, standards and rules designed by the Cloud Service Owners / Architects (Platform) role.	Current
Operators (Security)	Who manages the operations security tasks and their control in respect of organization security standards and their control in respect of policy, standards and rules designed by the Cloud Service Owners / Architects (Security) role.	Current
Operators (Compliance)	Who manages the compliance security tasks and their control in respect of organization regulations/normative and their control in respect of policy, standards and rules designed by the Cloud Service Owners / Architects (Compliance) role.	Current
Operators (Networking)	Who manages the operations tasks of service under this scenario and their control in respect of policy, standards and rules designed by the Cloud Service Owners / Architects (Networking) role.	Current
Operators (Storage)	Who manages the operations tasks of service under this and their control in respect of policy, standards and rules designed by the Cloud Service Owners / Architects (Storage) role.	Current
Operators (Identity)	Who manages the operations tasks of service under this scenario and their control in respect of policy, standards and rules designed by the Cloud Service Owners / Architects (Identity) role.	Current
Operators (Compute)	Who manages the operations tasks of service under this scenario and their control in respect of policy, standards and rules designed by the Cloud Service Owners / Architects (Compute) role.	Current
Operators (Containers)	Who manages the operations tasks of service under this scenario and their control in respect of policy, standards and rules designed by the Cloud Service Owners / Architects (Containers) role.	New (Cloud)
Billing Admins	Who manages billing tasks as making purchases, managing subscriptions, support billing tickets, and monitoring service health (for instance Office activation report).	New (Cloud)

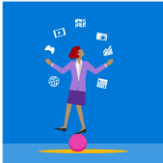
(*): The **New (Cloud)** value refers to those roles introduced with cloud world, while the **Current** value refers to those roles already in place in the On-Premise scenario too.



Organizational Scale Cloud Operations



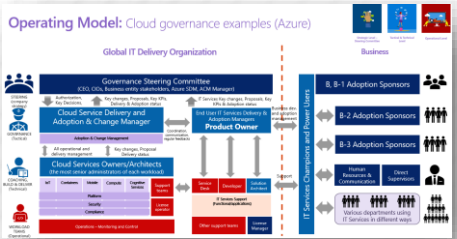
Strategic Level –
Steering Committee



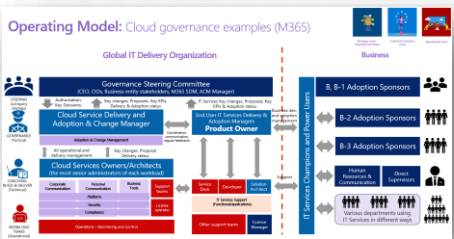
Tactical & Technical
Level



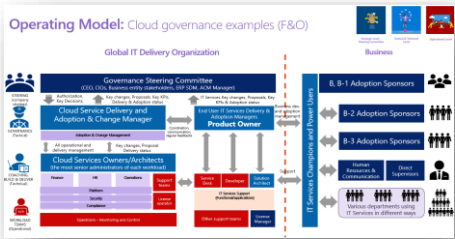
Operational Level



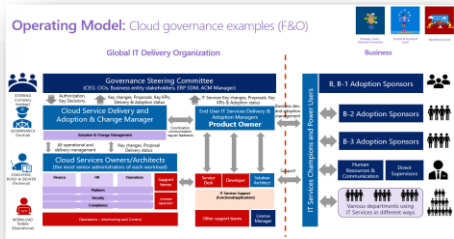
Azure



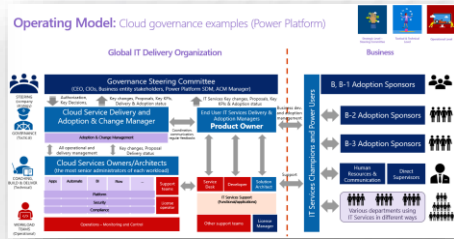
M365



D365 CE



D365 F&O



Power Platform

Cloud Competence Center

Strategic Level

- Committee Chairman & members
- Financial Management Representative
- Business Representative
- IT Management Representative
- Security Authority
- Compliance Authority
- ...

Tactical & Technical Level

- Cloud Service Manager
- Cloud Architect
- Cloud Operations Owner
- Product Owner
- IT Service Champs & Power Users
- Communication Lead
- ...

Operating Level

- Cloud Administrator
- Cloud Operators
- Cloud Support Resources
- Service Desk Resources
- Monitoring & Control Units
- Support Team Infrastructure
- ...

Empower the business

Drive and delegate Operations



Building Technical Skills

- Organizational and environmental (technical) readiness can require new [skills for technical and nontechnical contributors](#).
- Depending on the motivations and organizational outcomes that are associated with a cloud-adoption effort, leaders may need to establish new organizational structures or virtual teams (v-teams) to facilitate various functions.
- Follow the online documentation links from the previous slides to meet these desired outcomes:
 - Align your organization
 - Organization alignment exercises
 - Establish teams
 - Break down silos and fiefdoms.
- Find learning modules/paths and certification information for Azure on Microsoft Learn : <https://docs.microsoft.com/en-us/learn/azure/>





**TIME FOR
REVIEW**

- Cloud Adoption Framework
- Roles in The Cloud
- Cloud Operations Team
- Azure RBAC and Azure AD Roles
- Role Charts
- Cloud Operating Model

THANK YOU!



Appendix

Roles Library for Azure AD

Global Administrator



Global
Admin

Description



Has unlimited access to all management features and most data in all admin centers.

Responsibilities



- Buy licenses
- Configure any tenant service:
 - Exchange
 - SharePoint
 - Teams
 - OneDrive
 - Security
 - Compliance
 -
- Manage other administrators
- Define the tenant policy usage and consumption
- Create, delete, and update any cloud objects as:
 - application, administrative units, policies,
 - roles, assignments, devices, settings,
 - subscriptions, users, features,
 - etc...

Tips



- Must be limited to a few people in your organization.
- This is role must be on the IT side.

Area



- Global

Scope



- Tenant

Process involvement



- Incident Management
- Change Management
- Operations / Configurations
- Monitoring
- Management of escalations to Microsoft
- Billing Management
- Service Catalog Management
- Service Level Management

General comments



- He's not a Technology administrator
- More service owner oriented

Operating Model












- Tactical / Technical Level



Billing Administrator



Billing
Admin

Description					
Makes purchases, manage subscriptions, manage service requests and monitors service health.					
Responsibilities		Tips			
<ul style="list-style-type: none">• Can perform actions related to the billing• Buy / Assign licenses• Must ensure Capacity Planning for licenses• Read and configure service health in the Microsoft 365 admin center AND Azure portal• Create and manage support tickets in the Microsoft 365 admin center AND Azure portal• Update basic properties for the organization• Read basic properties on all resources in the Microsoft 365 admin center		<ul style="list-style-type: none">• Must be limited to a few people in your organization• This role can be hosted in a team which is not part of IT (i.e. Finance, Accounting...)			
				Area	
				<ul style="list-style-type: none">• Other	
Scope					
<ul style="list-style-type: none">• Tenant					
Process involvement			General comments		
<p>Related to billing only scenario:</p> <ul style="list-style-type: none">• Incident Management• Operations• Management of escalations to Microsoft• Billing Management			<ul style="list-style-type: none">• A subset of the Global Admin dedicated to the billing		
Operating Model					
<ul style="list-style-type: none">• Operational Level					



Helpdesk Administrator



Helpdesk
Admin

Description



Need to do some actions only for non-admin users and users assigned the Directory reader, Guest inviter, Helpdesk admin, Message Center reader, or Reports reader.

Responsibilities



- Reset passwords
- Force users to sign out
- Read and configure service health in the Microsoft 365 admin center AND Azure portal
- Create and manage support tickets in the Microsoft 365 admin center AND Azure portal
- Force sign-out by invalidating user refresh tokens
- Reset passwords for all users
- Read BitLocker keys
- Read basic properties on all resources in the Microsoft 365 admin center

Tips



- Applicable to Help Desk and/or Service Desk Lead.

Area



- Identity

Scope



- Tenant

Process involvement



- Incident Management
- User Management
- Management of escalations to Microsoft

General comments



- Helpdesk admins can change passwords for people who might have access to sensitive, private, or critical information.
- Changing the password of a user provides the potential to assume that user's identity and permissions.

Operating Model










- Operational Level



Service Administrator



Service
Admin

Description				
Called as Service Support Admin.				
Responsibilities		Tips		
<ul style="list-style-type: none">• Allows to read information / configurations of the tenant• Could be useful for teams in charge of incident resolution to help them• Read and configure service health in the Microsoft 365 admin center AND Azure portal• Create and manage support tickets in the Microsoft 365 admin center AND Azure portal• Read all network performance properties in the Microsoft 365 admin center• Read basic properties on all resources in the Microsoft 365 admin center		<ul style="list-style-type: none">• It's the unique role with opening and managing permission.• Assign this role as an additional role to admins or users for giving this actions enablement.		
Process involvement			General comments	
		<ul style="list-style-type: none">• Incident Management• Operations• Management of escalations to Microsoft	<ul style="list-style-type: none">• A « read-only » role	
Operating Model				
			<ul style="list-style-type: none">• Operational Level	



Message Center Reader



Message
Center
Reader

Description



Read and shares regular messages in Message Center, gets email notifications, has read-only access to users, groups, domains and subscriptions.

Responsibilities



- Monitor message center notifications
- Get weekly email digests of Message Center posts and updates
- Share message center posts excluding security messages
- Have read-only access to Azure AD services, such as users and groups

Tips



- It can fall within Monitoring or Operations Management team responsibilities

Area



- Read-Only

Scope



- Tenant

Process involvement



- Incident Management
- Operations
- Management of escalations to Microsoft
- Change Management

General comments



- A « read-only » role.
- This role doesn't give permission to read data privacy messages.
- Only the Message Center privacy reader and the Global admin can read data privacy messages.

Operating Model



- Operational Level



Message Center Privacy Reader



Message
Center Privacy
Reader

Description



Access to data privacy messages in Message Center, gets email notifications, has a read-only access to users, groups, domains and subscription.

Responsibilities



- Permission to read all notifications in the Message Center:
 - including data privacy messages
 - excluding security messages
- Get email notifications related to data privacy
- Share message center posts
- View groups, domains, and subscriptions
- Open and manage service requests

Tips



- Must be limited to a few people in your organization.
- This role can be hosted in a team which is not part of IT (i.e. Security OU).

Area



- Read-Only

Scope



- Tenant

Process involvement



- Incident Management
- Operations
- Management of escalations to Microsoft
- Change Management

General comments



- A « read-only » role.
- Only users assigned the Message Center privacy reader role or the Global admin role can read data privacy messages.

Operating Model



- Operational Level



Users Administrator



User
Admin

Description



Manage user lifecycle from creation to dismissal, license assignment, update password policy, monitor service health .

Responsibilities



- Add users and groups
- Assign licenses
- Manage most user properties, except username
- Create and manage user views
- Read and configure service health in the Microsoft 365 admin center AND Azure portal
- Create and manage support tickets in the Microsoft 365 admin center AND Azure portal
- Update password expiration policies
- Manage usernames
- Delete and restore users
- Reset passwords
- Force users to sign out by invalidating refresh tokens
- Update (FIDO) device keys

Tips



- Must be limited to a few people in your organization.
- This role must be on the IT side.

Area



- Identity

Scope



- User

Process involvement



- Incident Management
- Operations
- Management of escalations to Microsoft

General comments



- Consider it if you synchronize users between M365 and On-Prem Active Directory,
- The existing process to manage users (and their attributes) in your existing Active Directory should only be updated to match new M365 requirements

Operating Model



- Tactical / Technical Level



Password Administrator



Password
Admin

Description



Reset passwords for non-admin users and users assigned the Directory reader role, Guest inviter role, and other Password admins.

Responsibilities



- Reset passwords for all users
- Read basic properties on all resources in the Microsoft 365 admin center

Tips



- Must be limited to a few people in your organization.
- This role must be on the IT side.
- Role can delegate to Help Desk and /or Service Desk only if it's an internal function.

Area



- Identity

Scope



- User

Process involvement



- Incident Management
- Operations
- Management of escalations to Microsoft

General comments



- Can change passwords for people who might have access to sensitive, private, or critical information.
- Changing the password of a user provides the potential to assume that user's identity and permissions

Operating Model



- Operational Level



Compliance Administrator



Compliance
Admin

Description



Manage regulatory requirements and eDiscovery cases, maintains data governance for locations, identities and apps.

Responsibilities



- Help your organization stay compliant with any regulatory requirements
- Manage eDiscovery cases
- Maintain data governance policies across Microsoft online locations, identities, and apps
- Manage all aspects of Microsoft Compliance Manager
- Read all properties in entitlement management in Azure AD
- Read basic properties on all resources in the Microsoft 365 admin center
- Read and configure service health in the Microsoft 365 admin center AND Azure portal
- Create and manage support tickets in the Microsoft 365 admin center AND Azure portal
- Set secondary roles where they are present

Tips



- Must be limited to a few people in your organization.
- This role can be hosted in a team which is not part of IT (i.e. Compliance, Governance OUs).

Area



- Security & Compliance

Scope



- Compliance

Process involvement



- Incidents & Problem Management
- Operations / Configurations
- Management of escalations to Microsoft
- Monitoring (technical & usage)
- Change Management
- Knowledge Management
- L1 & L2 steering

General comments



- Ensure that company policies and procedures are being followed, and that behavior in the organization meets the minimum company standards of conduct and disposition.
- He's not a Technology administrator

Operating Model



- Tactical / Technical Level



Customer Lockbox Access Approver



Customer
Lockbox Access
Approver

Description



Manage Customer Lockbox requests, can turn Customer Lockbox capability on or off.

Responsibilities



- Manage Customer Lockbox requests for your organization
- Turn the Customer Lockbox feature on or off
- Approve and deny requests
- Receive email notifications for requests

Tips



- Must be limited to a few people in your organization.
- This role must be on the IT side.
- This role cannot delegate to Help Desk or Service Desk people.

Area



- Security & Compliance

Scope



- Security

Process involvement



- Incidents & Problem Management
- Management of escalations to Microsoft

General comments



- Keep track of and protect your organization's data across Microsoft online locations
- Get insights into issues to help mitigate risk

Operating Model



- Operational Level



User Access Administrator (RBAC)



User Access
Admin

Description



Let's you manage user access to Azure resources.

Responsibilities



- Manage authorization
- Read resources of all types, except secrets.
- Create and update a support ticket

Tips



- Create a custom role only if built-in RBACs don't address your need.
- Role can be assigned to user in every organization unit within the company.

Scope



- Root Management Group
- Management Group
- Subscription
- Resource Group
- Resource

Process involvement



- Access Management
- Incident Management
- Monitoring

General comments



Operating Model



- Operational Level

