Cloud Adoption Framework - Governance Overview

Abdul Kazi

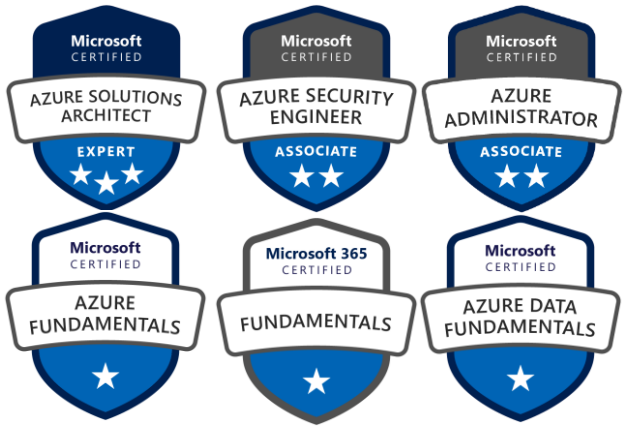
Thursday,
Feb 24th, 2022
8:00 PM UTC

Join Abdul for a session on Governance within the Cloud Adoption Framework.

LDNA

Limerick DotNet-Azure User Group

@LimerickDotNet



Abdul Kazi

abdulkazi

BLOG www.abdulwkazi.com

abdulwkazi

Cloud Adoption Motivations

Why is the company adopting the cloud?
More than one motivation is common in most cloud adoption efforts

Critical Business Events

- Data center exit
- Mergers, acquisition or divestiture
- Reductions in capital expenses
- End of support for mission critical technologies
- Regulatory compliance, data sovereignty requirements
- Reduce disruptions and improve IT stability

Migrate Motivations

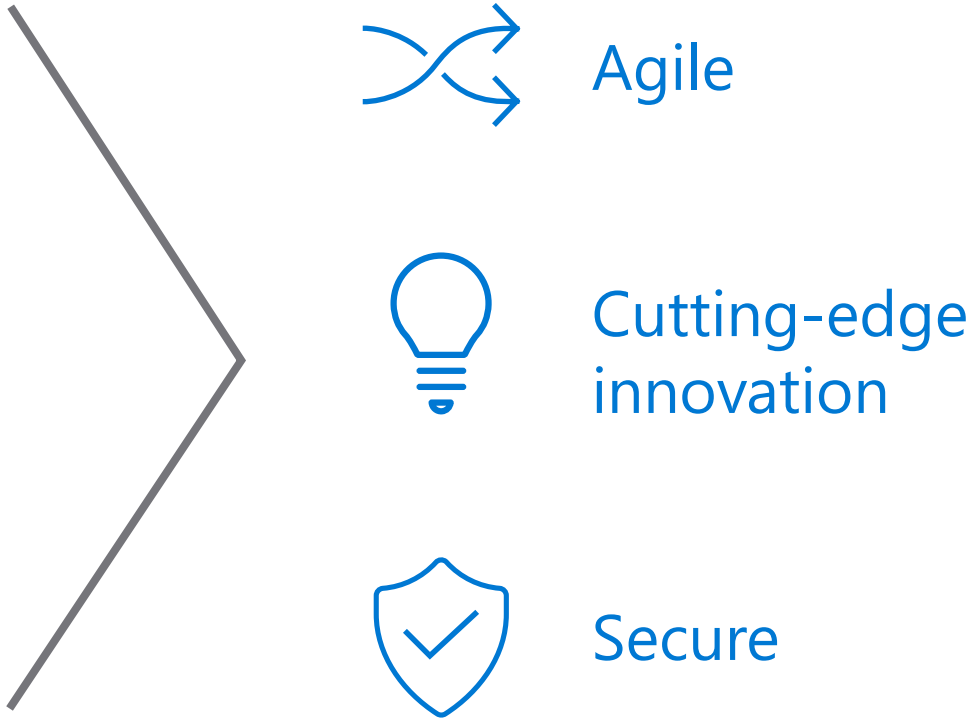
- Cost Savings
- Reduction in vendor or technical complexity
- Optimization of internal operations
- Increase business agility
- Prepare for new technical capabilities
- Scale to meet market demands
- Scale to meet geographic demands

Innovation Motivations

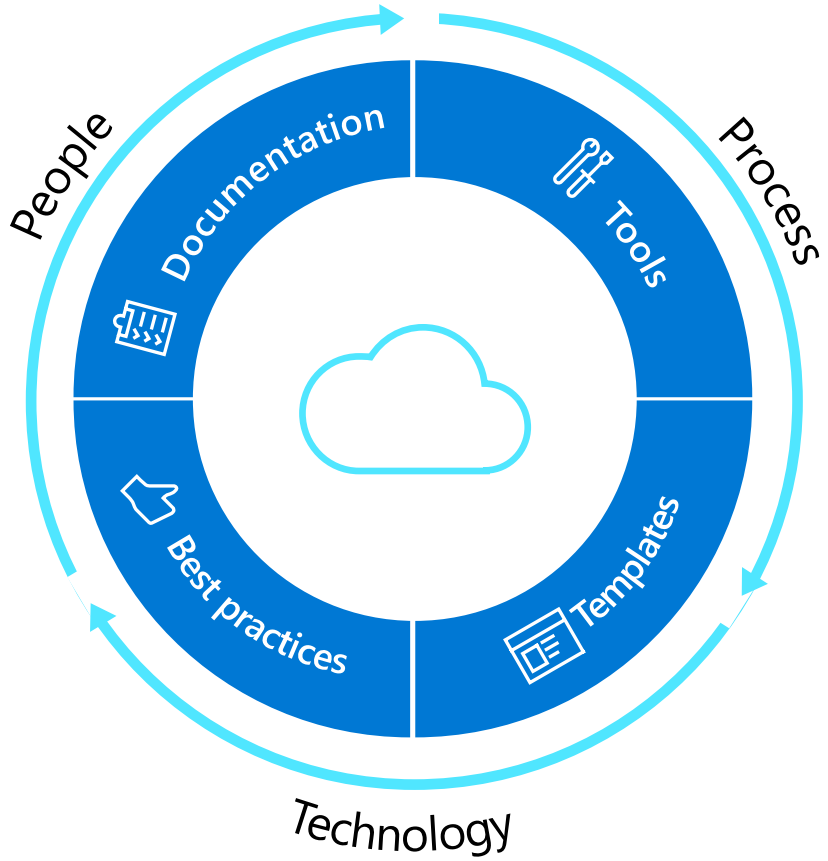
- Prepare for new technical capabilities
- Build new technical capabilities
- Scale to meet market demands
- Scale to meet geographic demands
- Improve customer experiences / engagements
- Transform products or services
- Disrupt the market with new products or services

The value of creating cloud-ready environments

- Aligned to business priorities
- Cloud-design considerations
- Adapted for cloud operating model
- Ready for cloud applications
- Adaptable to grow and expand
- Compliant

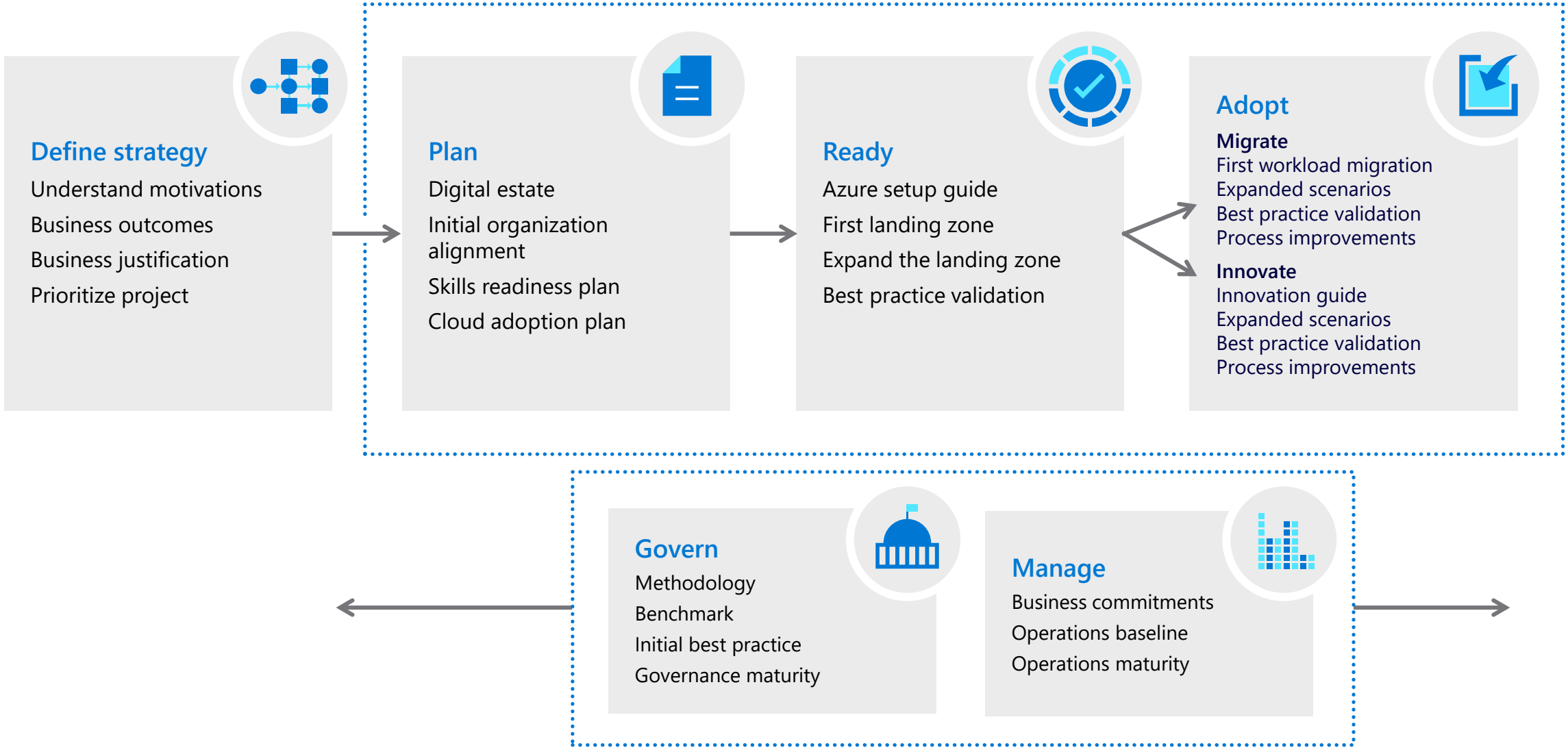


Microsoft Cloud Adoption Framework for Azure



Align **business, people and technology strategy** to achieve business goals with **actionable, efficient, and comprehensive** guidance to deliver fast results with control and stability.

Microsoft Cloud Adoption Framework for Azure



The major drivers for IT Governance

Keep risk at acceptable levels

Maintain availability to systems and services

Consistently apply policy and audit compliance

Protect customer data

Modernization

Improving customer and employee experiences

Transformation

Evolving how businesses operate and interact with the market

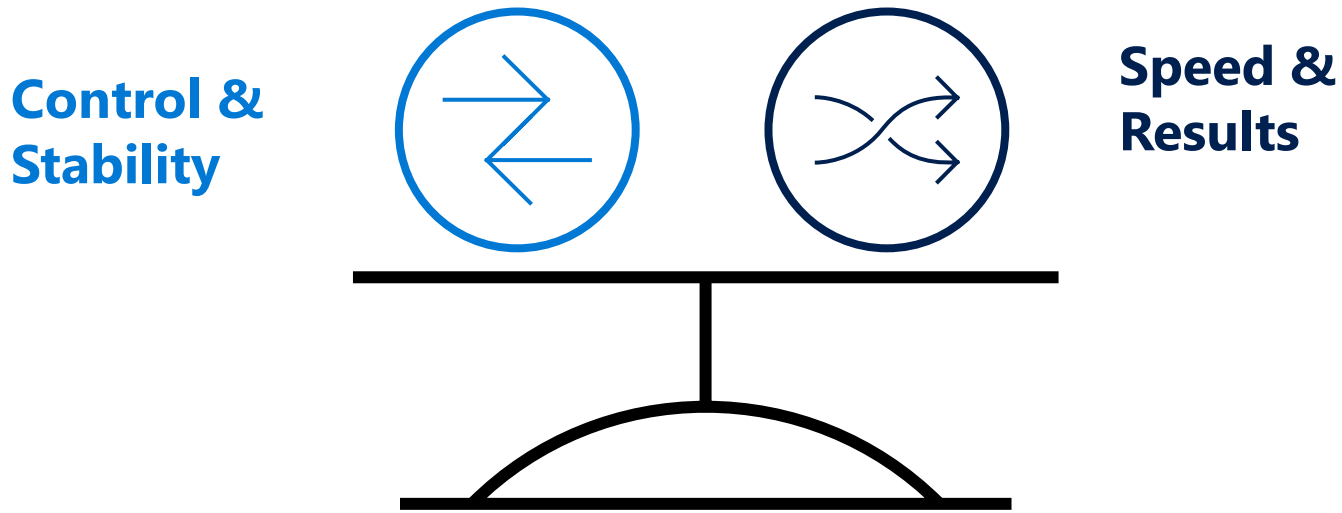
Growth

Scaling products and services to meet ever growing business needs

Business Returns

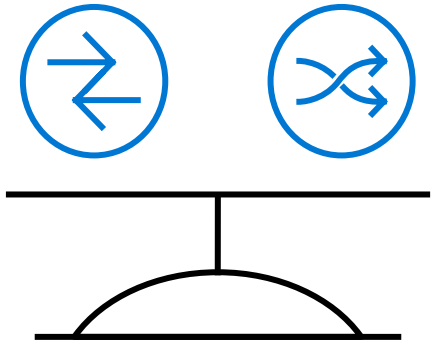
IT must rapidly produce measurable business returns to stay relevant

Objective of this model: Create balance



Why is Governance Important?

Transformation



Risk mitigation

- Maintaining full compliance
- Creating better cost visibility and control
- Improving security posture
- Being agile—to support scale

Who is responsible for monitoring? support? And operations?

Which services should be migrated to Azure?

What roles & responsibilities must be defined?

What security measures should I consider?

What are the core processes needed for service management?

How do I ensure a balance between innovation, cost and agility?

What organizational changes are needed?

What key capabilities I must develop?

Azure governance building blocks?

Assessment - **Cloud Adoption Framework Governance Benchmark Tool**

https://cafbaseline.com/

CAF Governance Model

Envision an end state – and incrementally build trust and confidence.

Govern

Define corporate policy

Business risks

Document evolving business risks and the business' tolerance for risk, based on data classification and application criticality

Policy & compliance

Convert risk decisions into policy statements to establish cloud adoption boundaries

Process

Establish processes to monitor violations and adherence to corporate policies.

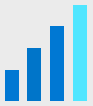
Five disciplines of cloud governance

Cost management

Evaluate & monitor costs, limit IT spend, scale to meet need, create cost accountability

Security baseline

Ensure compliance with IT security requirements by applying a security baseline to all adoption efforts



Resource consistency

Ensure consistency in resource configuration. Enforce practices for on-boarding, recovery, and discoverability

Identity baseline

Ensure the baseline for identity and access are enforced by consistently applying role definitions and assignments

Deployment acceleration

Accelerate deployment through centralization, consistency, and standardization across deployment templates

Governance funnels corporate policy changes into five actionable disciplines – **enabling your organization to modernize and reach business goals.**

https://aka.ms/adopt/Gov

Making Governance Actionable with Azure Native Tools

Cloud Native Tools

Cost Management

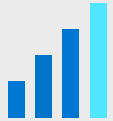
- Azure Blueprints
- Azure Policy
- Azure Cost Management
- Azure Advisor

Security Baseline

- Azure Blueprints
- Azure Policy
- Azure Security Center
- Azure Sentinel
- Threat Protection

Identity Baseline

- Azure Blueprints
- Azure RBAC
- Azure AD
- Azure AD B2B
- Azure AD B2C
- Directory Federation
- Directory Replication



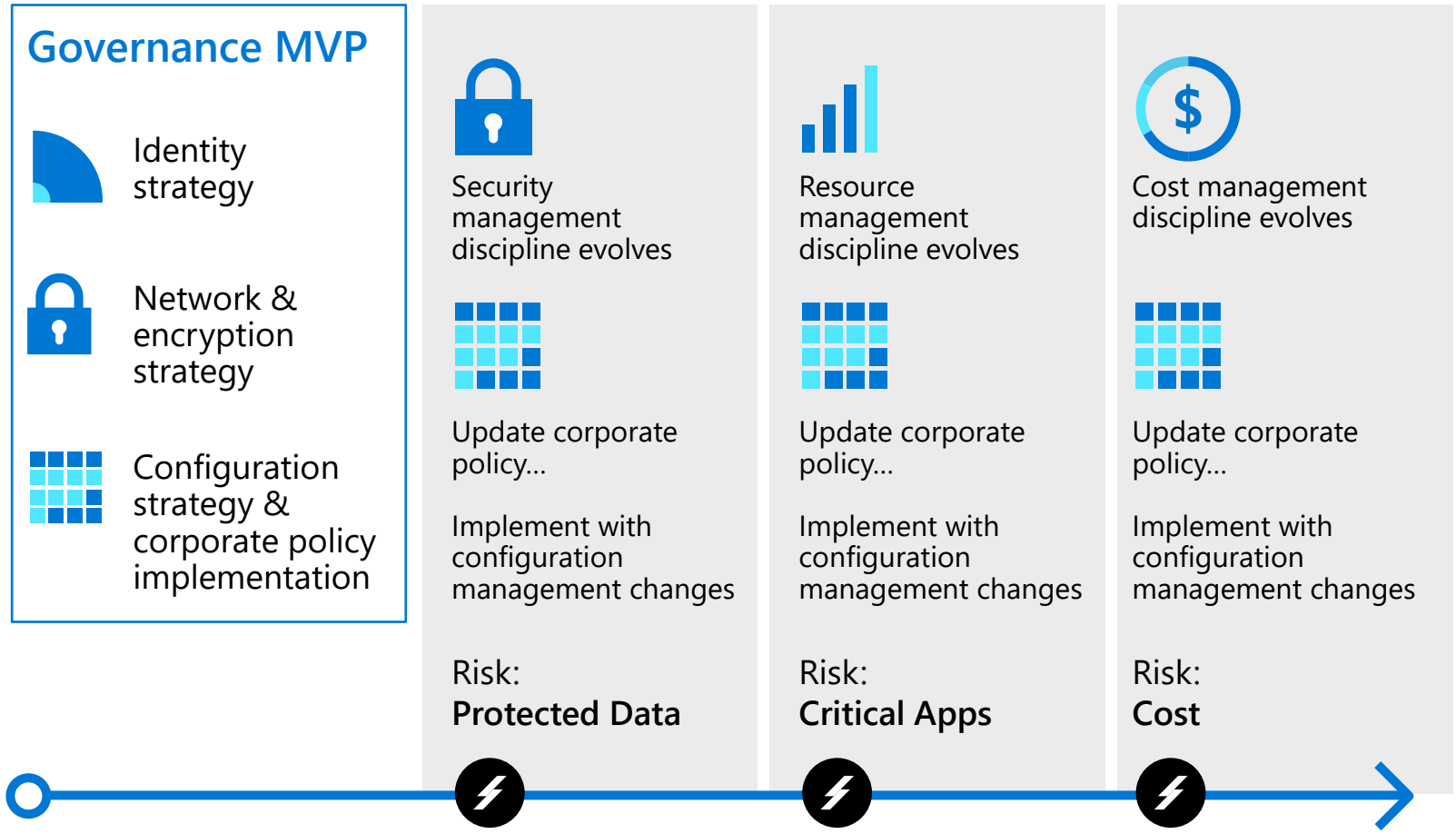
Resource Consistency

- Azure Blueprints
- Azure Policy
- Azure Monitor
- Change Tracking
- DSC
- Update Management
- Automation

Deployment Acceleration

- Azure Blueprints
- Azure Policy
- Resource Tagging
- ARM Templates
- Azure DevOps
- Azure Site Recovery
- Azure Backup
- Azure Automation

Executing Incremental Governance



Adoption timeline will trigger **risks** along the journey

Build the Governance MVP

Standard enterprise	Complex enterprise
1. Customers or staff reside largely in one geography	1. Customers or staff reside in multiple geographies or require sovereign clouds
2. Business units share a common IT infrastructure	2. Multiple business units that do not share a common IT infrastructure
3. Single IT budget	3. Budget allocated across business units and currencies
4. Capital expense-driven investments are planned yearly and usually cover only basic maintenance	4. Capital expense-driven investments are planned yearly; often include maintenance and refresh cycles of 3-5 years
5. Datacenter or third-party hosting providers with fewer than five datacenters	5. Datacenter or third-party hosting providers with more than five datacenters
6. Networking includes no WAN; or 1-2 WAN providers	6. Networking includes complex network or global WAN
7. Identity is a single forest, single domain	7. Identity consists of multiple forests, multiple domains
8. Cost Management (cloud accounting) showback model – billing is centralized through IT	8. Cost Management (cloud accounting) chargeback model – billing can be distributed through IT procurement
9. Security Baseline – protected data: company financial data and IP. Limited customer data. No third-party compliance requirements.	9. Security Baseline (protected data) – Multiple collections of customers' financial and personal data

Cloud Governance Team and Functions

A cloud governance team evaluates and manages risk tolerance, identifies high-risk areas for business, and converts risks into governing corporate policies.

- Ensures cloud-adoption risks and risk tolerance are properly evaluated and managed.

- Identifies risks that can't be tolerated by the business, and it converts risks into governing corporate policies.

Cloud Governance Team

- Review Govern module of Cloud Adoption Framework
- Complete the governance benchmark
- Implement the governance MVP approach
- Continuously improve governance maturity

Cloud Governance Team

Align with other teams to

- Review your company's strategy and plan
- Review your company's cloud adoption plan
- Review the operation team's operations management workbook

Establish cadence with teams that aligns with

- Release and planning cycles.
- The cloud strategy team to review risks of the next wave of adoption and gauge the team's level of tolerance for risks.
- Review and iterate.

Cost Management

Establish controls and processes to ensure proper allocation of cost across business units, implement cost guardrails, and analyze the cost of applications.

Define

- Enterprise Enrollment Hierarchy Process and RACI Azure Cost Management Budgets and Alerts + RACI
- Cost Management RBAC Model

Define Cost Management Policies

- Tagging
- Allowed VM SKUs
- Allowed Storage SKUs
- Allowed Networking SKUs
- Allowed Database SKUs

Security Baseline

Establish policies to protect your network, assets, and data – residing on cloud provider platform(s).

Document risks, business tolerance, and mitigation strategies related to the security of:

- **Data and assets:** develop clear, simple, and well-communicated guidelines to identify, protect, and monitor the most important data assets
- **Network:** control and monitor any allowed communication between on-premises environment and cloud workloads.

Implement these best practices for corporate policy:

- **Network requirements:** on-premises networks must be secured against potential unauthorized access from cloud-based resources.
- **Hybrid identity strategies:** a key factor in structuring cloud-based identity services is the level of integration required with existing on-premises identity infrastructure.
- **Encryption:** encryption mechanisms vary in cost and complexity, and both technical and policy requirements and can influence decisions on how encryption is applied and how to store and manage critical secrets and keys
- **Security Baseline policies:** processes that manage updates to security policy based on inputs from stakeholders. (e.g., initial risk assessment and planning, deployment planning and testing, and quarterly review and planning)

Resource Consistency

Implement the foundation for governance best practices –
with correct resource organization.

Define Azure Management Groups & Subscriptions model and RACI

- To reflect security, operations and business/accounting hierarchies
- To group similar resources into logical collections

Define resource consistency roles & responsibilities

- To further group applications or workloads into deployment and operations units

Define Resource Consistency Policies

- Naming Conventions
- Tagging
- Allowed Locations
- Allowed Resource Types
- Allowed Extensions
- Auditing

Identity Baseline

Protect your data and assets in the cloud –
implementing identity management and access control.

Define Azure RBAC Model

- Using RBAC can 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 an Azure subscription or resources, only certain actions with narrow scope can be allowed.

Define Azure Access Management Process and RACI

- Several options are available for managing identity in a cloud environment which vary in cost and complexity.
- A key factor in structuring your cloud-based identity services is the level of integration required with existing on-premises identity infrastructure.

Operationalize Azure Privileged Identity Management

- Cloud-based identity management is an iterative process.

Deployment Acceleration

Establish policies to govern asset configurations or deployments – manual, or automated through DevOps best practices.

The DevOps practices in this discipline include:

Infrastructure as code

- Stand up environments in the fastest means possible.
- Remove the human element and reliably and repeatable deploy every time.
- Improve environment visibility and improve developer efficiency
- Store infrastructure definitions alongside application code.

Continuous integration and continuous deployment

- Accelerate delivery through automation
- Simple and easy to use
- Global community for actions

Azure services that enable deployment acceleration include Azure Blueprints

Deploy and update cloud environments in a repeatable manner using composable artifacts

Sample Policies

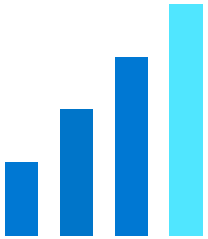
Cost Management

- Modify CostCenter Tag & its value from Resource Group
- Modify CostCenter Tag to Resource Groups
- For tracking purposes, all assets must be assigned to an application owner within one of the core business functions.
- When cost concerns arise, additional governance requirements will be established with the finance team.
- Allowed Azure Region for Resources and Resource Groups
- Allowed Azure VM SKUs

Security Baseline

- All deployed assets must be categorized by criticality and data classification.
- All protected data must be encrypted when at rest.
- Network subnets containing protected data must be isolated from any other subnets. Network traffic between protected data subnets is to be audited regularly.
- All connections between the on-premises and cloud networks must take place either through a secure encrypted VPN connection or a dedicated private WAN link.
- No public facing web site backed by IaaS should be exposed to the internet without DDoS.
- Governance tooling must audit and enforce network configuration requirements defined by the Security Baseline team.
- Trends and potential exploits that could affect cloud deployments should be reviewed regularly by the security team to provide updates to Security Baseline tooling used in the cloud..

Resource Consistency

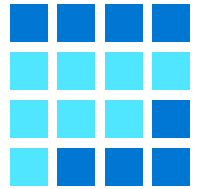


- All deployed assets must be categorized by criticality and data classification.
- Subnets containing mission-critical applications must be protected by a firewall solution capable of detecting intrusions and responding to attacks.
- Governance tooling must audit and enforce network configuration requirements defined by the Security Management team.
- Governance tooling must validate that all assets related to mission-critical apps or protected data are included in monitoring for resource depletion and optimization.
- Governance tooling must validate that the appropriate level of logging data is being collected for all mission-critical applications or protected data.
- Governance process must validate that backup, recovery, and SLA adherence are properly implemented for mission-critical applications and protected data.

Identity Baseline

- All assets deployed to the cloud should be controlled using identities and roles approved by current governance policies.
- A least-privilege access model will be applied to any resources involved in mission-critical applications or protected data.
- Elevated permissions should be an exception, and any such exceptions must be recorded with the cloud governance team. Exceptions will be audited regularly.
- All groups in the on-premises Active Directory infrastructure that have elevated privileges should be mapped to an approved RBAC role.
- All accounts are required to sign in to secured resources using a multi-factor authentication method.
- Deployment of any applications that require customer authentication must use an approved identity provider that is compatible with the primary identity provider for internal users.

Deployment Acceleration



- All assets deployed to the cloud should be deployed using templates or automation scripts whenever possible.
- Key metrics and diagnostics measures will be identified for all production systems and components.
- Operations will consider using monitoring and diagnostic tools in nonproduction environments such as Staging and QA to identify system issues before they occur in the production environment.
- Cloud governance processes must include monthly review with configuration management teams to identify malicious actors or usage patterns that should be prevented by cloud asset configuration.

Resources

Learn more about the Microsoft Cloud Adoption Framework and cloud management.

Microsoft Cloud Adoption Framework for Azure: Introduction
https://azure.microsoft.com/cloud-adoption-framework/

Microsoft Cloud Adoption Framework for Azure: Documentation
https://docs.microsoft.com/azure/cloud-adoption-framework/

Cloud management in the Cloud Adoption Framework
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/govern/methodology

Governance benchmark assessment
aka.ms/adopt/assess/govern

Enterprise Scale landing zone
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/