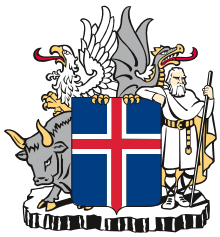


Governance Framework for Microsoft Azure in Iceland

Policies to utilize Microsoft Azure services in the Icelandic public sector.

V1.0 – Open: For Public distribution

12.09.2023

Content

1. General / Inngangur

Eftirfarandi skjal er unnið af fjármála- og efnahagsráðuneytinu og gefið út og samþykkt í október 2023 í útgáfu 1.0. Undirbúningur þess er samvinna margra ríkisaðila í formi vinnuhópa og rýni ásamt aðkomu erlendra ráðgjafa á sviði skýjalausna. Eigandi skjalsins er skrifstofa stjórnunar- og umbóta og eru breytingar og viðbætur skjalsins rýndar og samþykktar af arkitektúrráði Microsoft verkefnisins / ríkissamningsins.

Tilgangur skjalsins er að setja samræmda umgjörð um innkaup, umsjón og notkun Azure skýjaþjónustu Microsoft. Skjalið er liður í innleiðingu Öryggis- og þjónustustefnu um hýsingarumhverfi – stefnu um notkun skýjalausna og aðgerðaáætlun henni.

Með því að útbúa og innleiða samræmda umgjörð um Azure skýjaþjónustuna þar sem sama hönnun er innleidd oft næst að tryggja öryggisstig og stytta þróunar- og afhendingartíma nýrra vara hjá ríkisaðilum. Umgjörðin tryggir auk þess að uppsetningar verði samræmdar, hvort sem innleiðing og rekstur er í höndum miðlægs aðila, ríkisaðilans sjálfs eða er í höndum þjónustuaðila af einkamarkaði.

Mun þetta skjal verða hluti af heildstæðri umgjörð um högun upplýsingatækni ríkisins. Er það birt m.a. á:

- Island.is: Stefnur og skilmálar
- Stjórnarráðið: Verkefni – Upplýsingatæknimál ríkisins

Þar sem umsjónarviðmót skýjaþjónustu Microsoft er á ensku er meginmál þessa skjals á ensku til að tryggja að hugtakanotkun sé samræmd.

Útgáfa	Lýsing	Dags.
1.0	Fyrsta útgáfa	2023-10-04

In 2021 Iceland defined “Strategic Cloud Policies” for using and promoting public cloud services in Icelandic government and public sector organisations.

In 2022, The Icelandic Ministry of Finance and Economic Affairs launched an initiative to define the principles for utilization of Microsoft Azure services. During the project the following matters were defined as a Governance Framework for the use of governmental institutions of Iceland:

- Procurement policies: how Azure services are procured and what are the agreement models to be used
- Management architecture: what is the required management architecture (i.e. management groups, subscriptions, resource groups) when building up solutions to Azure and how they can be deployed
- Usage policies: what are the recommended and/or required technical policies (such as tagging and location) when using Azure services.

The main target for the Governance Framework is to have a ready framework and policies that can be utilized to shorten implementation time, reduce cost, standardize implementation and implement required cost and security controls of cloud platforms/projects deployed in Azure.

The “Strategic Cloud Policies” document is further referred to in this document as **Strategic Cloud Policies**.

1.1. Reasons for defining a Governance Framework

The reasons why the governance framework is defined are:

1. **Ease-of-use**

   Unifying the policies means that there are common, repeatable procedures which in turn lead to faster implementation of services, when there is a clear understanding on how and why to implement the services. When developed further, these common practicalities can be transformed in to Infra-as-Code and used with automated DevOps tools.

2. **Visibility**

   Increasing visibility to the Azure usage through chosen procurement models enables the Icelandic institutions to have a clear understanding to their costs and also grants visibility to the overall Azure usage for the entire Icelandic governmental agencies.

3. **Security**

   When agreed policies are put into action, they enable compliance auditing features and – if enforced – leads into ensured compliance in the environment for security, privacy and cost.

4. **Centralized assistance**

   Common policies enable solution partners to better assist each institution to use the Azure services efficiently as well as enabling inhouse teams to deploy and use the services faster.

2. Terminology

The following terms are used across this document:

- Agreement – the contract which is used to purchase Azure consumption
- Tenant – the Azure Active Directory instance
- Tenant Admin – the administrator of the Azure AD instance
- Tenant Operator – the entity operating the Azure AD instance
- Billing structure – used to describe the hierarchy of an agreement all the way to the Subscriptions in an contrual model
    - Billing account – Agreement that is used to purchase Microsoft products and services. Contains one or more departments and accounts. Invoice is created on this level.
    - Department – An optional way to group accounts into separate cost segments for the creation of budgets.
    - Account – Describes a singular owner. Account owner has the right to create and manage Subscriptions.
- Management group – the grouping used for management activities
- Subscription – a singular subscription
- Resource group – a group of technical resources that are combined into a single manageable entity
- Resource – a singular technical resource (such as a virtual machine)
- Role-Based Access Control (RBAC) – the rights for individual users and groups for the above components.

3. Procurement

Procurement consists of the following subjects:

1. Agreement model
2. Governance model.

The following sections describe the policies of above subjects.

3.1. Agreement model

In the **Strategic Cloud Policies**, the following statement is made:

> ***Use trusted purchase channels and be cost conscious***
>
> *Purchase cloud services from selected and shared public channels, and from cloud vendors that have been selected through a formal process. Be cost conscious and use public funds responsibly – only buy what you need at any given time. Allocate costs fairly in the cloud native way – always pay your own use – do not piggyback on others' costs.*

As the agreement and contractual model used has no impact on the governance and usage of Azure cloud services this chapter is redacted from the Open version of this document as these structures can change without any notice from Microsoft and/or Microsoft.

Agreement model is the actual contract that is used to procure the Azure services. There are multiple agreement models available from Microsoft as described in *Figure 1 - Microsoft Azure agreement models*.

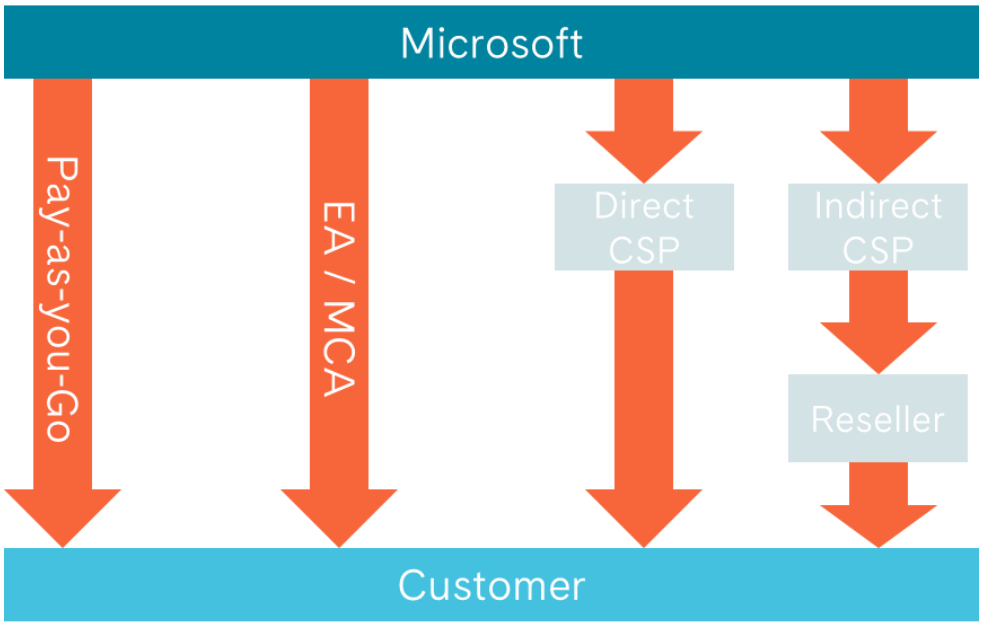


Figure 1 - Microsoft Azure agreement models

Abbreviations used in the Figure:

- *EA = Enterprise Agreement*
- *MCA = Microsoft Customer Agreement*
- *CSP = Cloud Solutions Provider (NCE)*
- *PayG = Pay-as-you-Go.*

3.2. Governance model

The governance model in the scope of procurement means:

a. Billing structure – the structure which is used when separating the consumption of different Institutions to ease the cost management activities inside the shared agreement.

b. the ownership and management of the Subscriptions (the management scope that connects consumption to an agreement).

The billing structure of Iceland is shown in *Figure 2 - Billing structure*. In essence, a *billing profile* is created for each Azure Tenant and the Tenant Operator of each Tenant will receive Billing Profile Owner rights for the relevant Billing Profiles. Under these Billing Profiles the *Invoice Sections* are created – under which the actual Subscriptions will be created.

***Billing profile** is used to separate the consumption under a single agreement to different invoices. Information such as payment methods and billing address are selected by Billing Profile.*

***Invoice Sections** may be used to divide costs to for example projects or different organization units. The Invoice Section is visible on the actual invoice.*

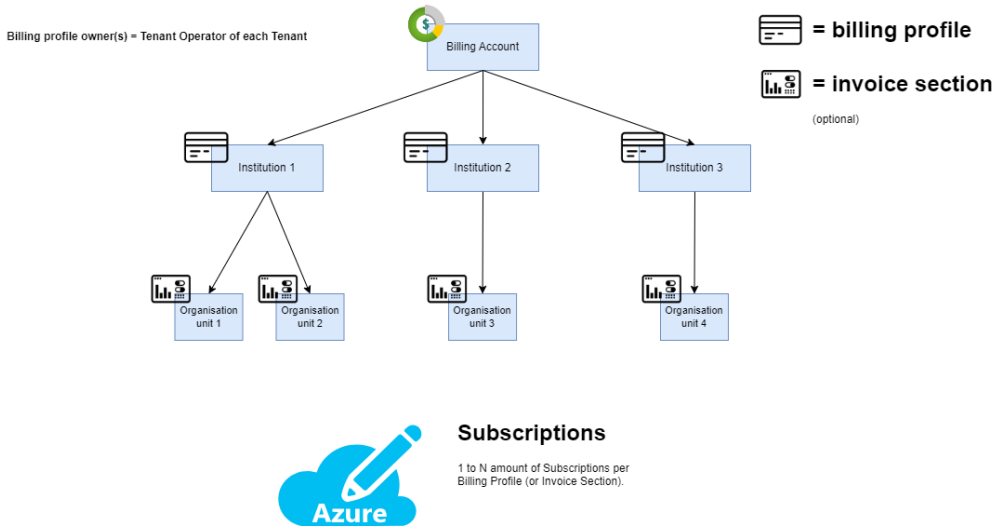


Figure 2 - Billing structure

3.3. Subscription ownership and management

There are three different types of Subscriptions, when it comes to the ownership and management model:

- Managed subscription, where a Tenant Operator offers a *turn-key* solution for the individual institutions.
- Unmanaged subscription, where an Institution takes responsibility of managing their own usage inside a subscription.
- Isolated environment, where an Institution takes full ownership of the environment from procurement and access management to individual resources.

The following table describes the responsibilities or different tasks in these three models.

TASK	MANAGED	UNMANAGED	ISOLATED
Procurement of Subscriptions	Central function	Central function	Central function
Management of Azure Active Directory	Tenant Operator	Tenant Operator	Institution
Creation, management and removal of Subscriptions	Tenant Operator	Tenant Operator	Institution
Adherence to the Icelandic policies (this document) on the Tenant and Subscription levels	Tenant Operator	Tenant Operator	Institution
Rights management inside a Subscription	Tenant Operator	Institution	Institution
Adherence to the Icelandic policies (this document) on Platform level	Tenant Operator	Institution	Institution
Azure resources creation, management and removal	Tenant Operator	Institution	Institution
Platform operations *	Tenant Operator	Institution	Institution
Platform development *	Tenant Operator	Institution	Institution

Adherence to the Icelandic policies (this document) on Solution level *	Institution	Institution	Institution
Solution operations *	Institution	Institution	Institution
Solution development *	Institution	Institution	Institution
Business alignment to each Institution's targets and re-quirements	Institution	Institution	Institution

* Platform and Solution refer to the division between *infrastructure components* and the *application-specific components* as shown in *Figure 3 - Division between Solution and Platform levels*.

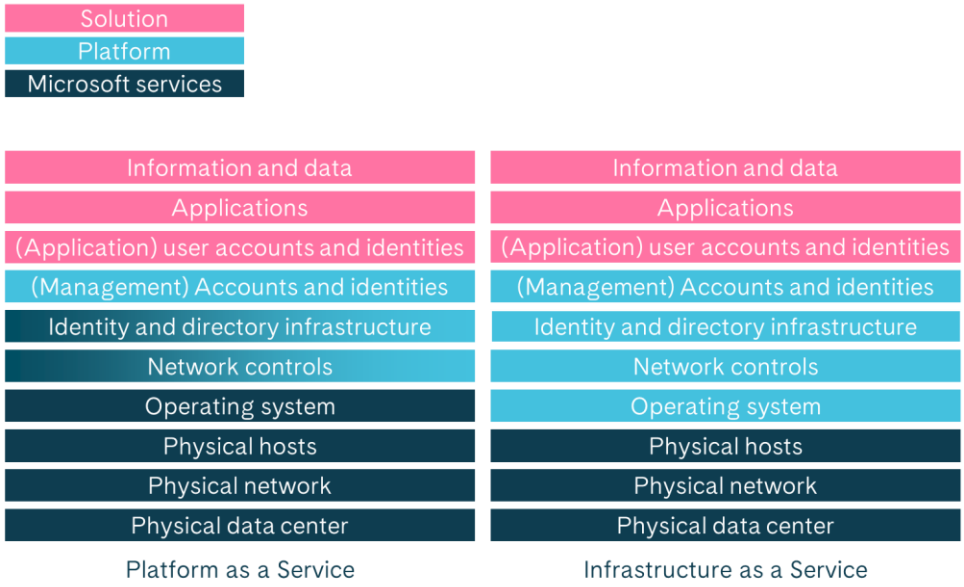


Figure 3 - Division between Solution and Platform levels

Managed subscription must be the default approach for all needs. Unmanaged subscription may be used when separately agreed so by the Institution and Tenant Operator in use cases, where the Institution will comply with the ownership requirements set in the table above. Isolated environments can only be used, where there is an approved use case (see: *3.3.1 Approved use cases for Isolated environment*) and the Architecture Board has approved the creation of an isolated environment.

3.3.1. Approved use cases for Isolated environment

This section describes the approved use cases for the Isolated environments. Isolated environments are in essence separate Azure Active Directory Tenants from the currently approved Tenants of Icelandic governmental Institutions.

The approved use cases for Isolated environments are the following:

1. The application that is created, is used for consumer purposes AND there is a need for Azure B2C (Business-to-Consumer) functionality
2. The Tenant is used for cross-border purposes, in essence the management of the environment is done by non-Icelandic entities in collaboration with Icelandic Institutions.

3.4. Policies

SCOPE	POLICY
Agreement	MCA is used by the Institutions.
Billing structure	Account is created for the Institutions as needed. 1-to-N Subscriptions are created under these Accounts.
Billing structure	Accounts are grouped into Departments based on the Azure Tenant
Billing structure	Department Administrator(s) are set based on Tenant Operator
Subscription ownership and management	A selection from three possible models is done by Institution: a) Managed subscription, where a Tenant Operator offers a turn-key solution for the individual Institutions b) Unmanaged subscription, where an Institution takes responsibility of managing their own usage inside a Subscription c) Isolated environment, where an Institution takes full ownership of the environment from procurement and access management to individual resources.

4. Management Architecture

Management Architecture is a compilation of Management Groups, Subscriptions, Resource Groups and Resources, which in turn create a hierarchy. This hierarchy can be used to:

1. Restricting and enabling administrative access, leading to secure environment with only necessary rights granted to each administrator.
2. Scoping policies, leading to organization-wide policy compliancy, while still allowing environment-specific policies related to for example automization.

Figure 4 - Management Architecture relationship describes the relationship between the different management objects.

Figure 4 - Management Architecture relationship

4.1. Policies

SCOPE	POLICY

Management Architecture	A top-level Management Group under the tenant Root Management Group must be created per Tenant, under which Management Group structure is created.
Management Groups	Create a “Platform” Management Group per Tenant to contain shared IT-related services such as networking hub, centralized log analytics workspaces etc.
Management Groups	Least privilege must be applied: Management Group structure must support the ideology of giving only the necessary administrative rights with ease-of-management ideology It is to be noted, that Role-Based Access Control may be used to grant rights to two distinct layers (control plane and data plane)*
Management Groups	Choose one of two design options depending on your management model (Managed & Unmanaged vs. Isolated) as described in *4.2 Design Examples*
Subscriptions	Every Subscription must have a named owner (individual, not a group)
Subscriptions	Subscriptions are created for workload separation: i.e. production, test/QA and development workloads are grouped into separate subscriptions. One of two options are used as described in *4.2.3 Subscription options*
Subscriptions	Using Azure Dev/Test Subscriptions for Development and Test environments should be considered, when the following services are used: Windows and Windows Server virtual machines, Azure SQL Database, Azure Logic Apps, Azure App Service, Azure Cloud Services instances, and Azure HDInsight instances **NOTE!** Requires Visual Studio subscriptions for all with access to the environment
Resource Groups	Resource Groups are created for each application and/or use that shares the same lifecycle. The workloads that are directly included in that application are placed into these Resource Groups.
Resource Groups	Shared workloads are grouped into applicable Resource Groups inside the Subscriptions, for example: Shared network resources are grouped into a “network” Resource Group Storage services (including databases) used by multiple applications are grouped into a “storage” Resource Group Backup-related resources (such as Recovery Vaults) are placed into a “backup” Resource Group

* Control plane and data plane are two layers, that can most easily be explained by using Storage Accounts as an example. When you have a Storage Account (*storageaccount-01*) that is hosting a file (*data1.txt*), accesses can be given on two levels:

1. Granting Contributor rights to *storageaccount-01* let's you manage the resource itself – for example adding file shares, modifying the size of the resource, but does not grant you access to the *data1.txt*
2. Granting Storage Blob Data Contributor rights to *storageaccount-01* let's you see and manage the file *data1.txt*, but does not grant you access to manage the resource.

4.2. Design Examples

4.2.1. Management Structure for Managed and Unmanaged Subscriptions

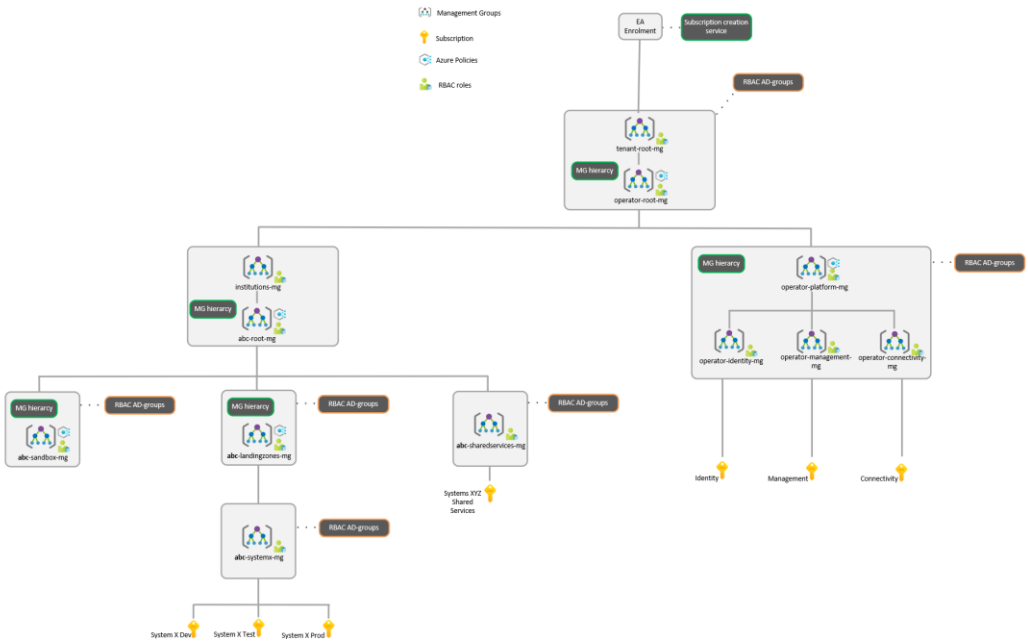


Figure 5 - Managed and Unmanaged Subscriptions model Management Structure

4.2.2. Management Structure for Isolated environment

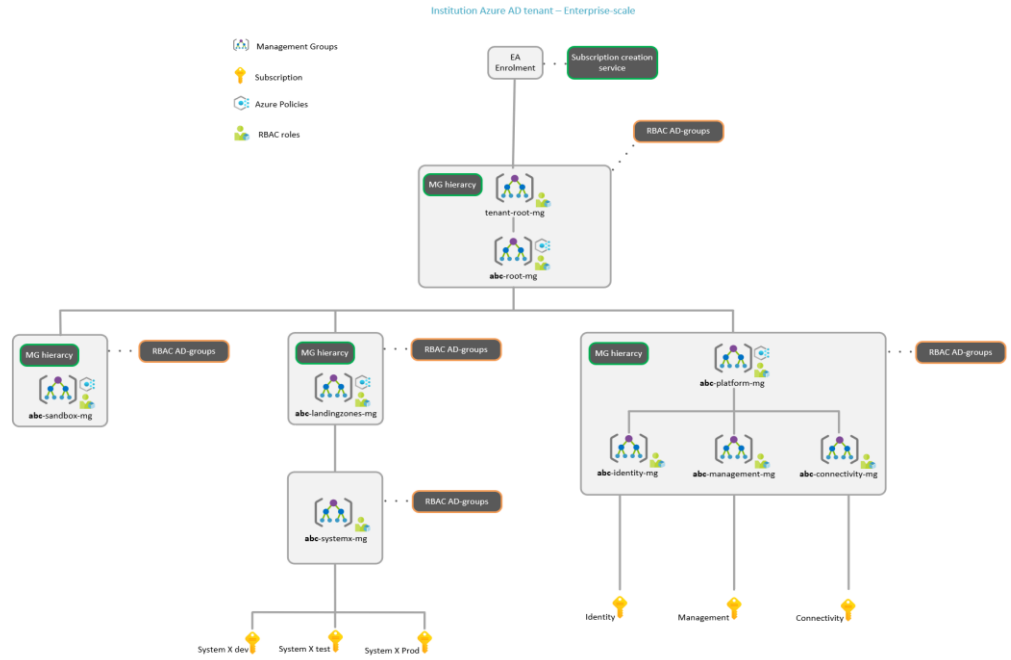
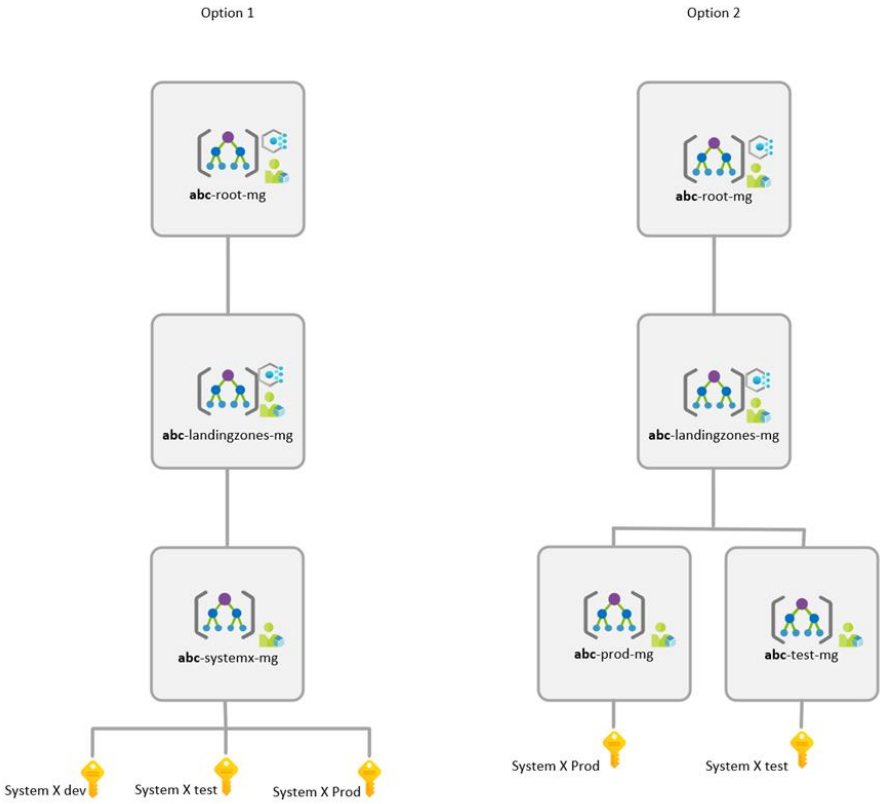


Figure 6 - Isolated environment model Management Structure

4.2.3. Subscription options



Option 1 is used when:

- When you know you have different 3rd parties or teams contributing to different applications. This structure makes it easier to assign RBACs for specific scope
- You want a simple hierarchy per application.

Option 2 is used when:

- When you want to bundle all your different environments under one Management Group
- Use this if you want to use different policy enforcements between environments
- When you can assign RBACs in a wider scope. As an example, if the environment in total is managed by a single party and there is no need to scope down the rights to each party separately (see Option 1).

5. Usage policies

It is important to have and follow a set of policies regarding the usage of Azure services. These policies have effect on – for example – manageability and costs. This section describes the usage policies set by Iceland.

5.1. Cost management

In the **Strategic Cloud Policies**, the following statement is made:

- *Strategic cloud policy 4.5: Make purchasing and ordering of general cloud platform services (capacity, technical services) easy and quick. Utilize cloud elasticity* ***to optimize the entire life cycle costs of the service****.*
- *Strategic cloud policy 4.6:* ***Costs of common governmental cloud services are allocated according to utilization.***
- *Strategic cloud policy 5.4: Utilize the elasticity of cloud services using iterative and experimentative development model. Publish and test often,* ***start small and expand according to growing needs****.*
- *Strategic cloud policy 6.3:* ***Measure and manage*** *your cloud suitability, continuity, security and* ***costs on a day-to-day basis****.*

The policies for Cost Management are stated in the following table.

SCOPE	POLICY
Ownership	The Resource owners and ultimately the Subscription owner is responsible of cost management procedures in the environment
Tool for cost management	Azure Cost Management is used for cost management activities. Subscription owners must have rights to see costs related to their Subscriptions.
Period of use	Resources must be kept running only when they are needed. Automated startup/shutdown processes are recommended for test and development workloads.
Review of used Resources	Resources must be reviewed regularly, in minimum once per three months, Unneeded resources must be removed.
Resource sizing	Begin with a minimum setup required for the use. Compare different kinds of resource types and product prizes prior to implementation.
Budgets	The Subscription owners are responsible of setting up budgets and cost alerting mechanisms.
Licensing	Use Microsoft Azure Hybrid Benefit (AHB) program when possible and when there are existing licenses available. AHB can be utilized with for example virtual machines and database services. Report and review the license use regularly.
Reservations	Use Azure Reservations as applicable. With Azure Reservation an up-front commitment of one or three year purchase is made, enabling a cost reduction of up to 72% compared to Pay-As-You-Go model.

5.2. Region

Region is important from three different angles:

1. Cost optimization: if you have interconnected resources in multiple Regions, traffic between them will cost more than if they are in a single Region.
2. High Availability: having business-critical resources in multiple Regions offers better SLA for the application
3. Data sovereignty: keeping data inside EU/ETA borders is important for non-public data.

The policies for used Regions are stated in the following table.

SCOPE	POLICY
Region	Primary Region to be used: North Europe Secondary Region for HA purposes: West Europe

5.3. Naming conventions

Naming conventions offer administrative users easy access to such information as:

- Owning Institution
- Resource type
- Associated application
- Environment (prod/test/dev)
- Azure region hosting it.

This in turn leads to less human errors, when the administrative users can see more easily which resources they are managing.

The generic naming conventions are stated in the following table.

COMPONENT	NAMING CONVENTION
Institution	Abbreviation (Orrakóði) of the institution owning the Subscription, Resource Group or Resource. Up to 5 characters long. Examples: *lsh* = National Hospital *fjr* = Ministry of Financial and Economical affairs Full list of Orra-codes shall be made available.
Resource type	Abbreviation for the resource type. The Microsoft best practices for abbreviations are found from here: https://learn.microsoft.com/en-us/azure/cloud-adoption-

	framework/ready/azure-best-practices/resource-abbreviations Examples: *rg* = Resource Group *vm* = Virtual Machine
Application or service name	Name of the application, workload or service. Examples: *sharepoint* *analytics*
Environment	Environment abbreviation: *prod* = production *dev* = development *test* = test *qa* = quality assurance
Region (optional)	Region, in case of a multi-region solution. Always have Region in the name, if other than the primary Region (North Europe). Examples: *neu* = North Europe *weu* = West Europe
Running number (optional)	For example 001, 002 or 003.

Note! Names are given in lowercase letters and are separated by hyphens (-).

So, a Resource Group owned by National Hospital, running a productional Sharepoint instance, may have the name of:

lsh-rg-sharepoint-prod-001.

Some resource types have limitations on the name length or used special characters. The naming convention for these resource types is stated in chapter *5.3.1 Exception to generic naming convention: Virtual Machines and Storage Accounts*.

5.3.1. Exception to generic naming convention: Virtual Machines and Storage Accounts

The following resource types have limitations on the name length or used special character:

- Virtual Machines: name can have a length of 2 to 15 characters
- Storage accounts: no special characters. Only numbers and letters are allowed.

Hence, the naming convention for these two resource types is stated in the following table.

COMPONENT	NAMING CONVENTION
Storage Account	Only numbers and letters. The name must not therefore contain hyphens. As an example a Storage Account owned by National Hospital, related to networks may have the name of: *lshstnetworkprod001*
Virtual Machine	Name can have a length of 2 to 15 characters. In essence the naming convention for virtual machines is: • Institution abbreviation (up to 5 characters) • Resource type (vm) • Application (up to 5 characters) • Environment (in one letter, see the list below*) • Running number (two numbers). As an example, a virtual machine owned by National Hospital related to networks may have the name of: *lshvmnetprod01*

** Environment abbreviations with Virtual Machines:*

- *p = production*
- *t = test*
- *d = development*
- *q = quality assurance / staging.*

5.4. Tagging

Tagging is a mechanism where resources are labeled with metadata (key – value pair). Tagging can be used for:

- Operations management purposes – tagging SLA, business criticality etc.
- Resource management – ownerships, environments, applications etc.
- Cost management – for example cost allocation.
- Classification of data – what confidentiality level is related to the workloads.
- Measuring compliancy with the policies set by the organization.
- Automation, such as start/stop procedures.

Tags are, in essence, there to help govern and manage the environment. They also help with filtering views – for example in Cost Management – enabling persons to see only the relevant workloads.

The policies for Tagging are stated in the following table.

TAG NAME	FORMAT AND/OR *EXAMPLE VALUE*	DESCRIPTION	NECESSITY
ApplicationName	Text Example: sharepoint	Application name	Mandatory
Env	prod dev qa test	Environment information	Mandatory
DataClassification	Open / Opin Protected / Varin Specially protected / Sérvarin Restricted / Afmörkuð	Data classification in English format, Icelandic provided for reference.	Mandatory
Orrakóði	The 3-5 letter Orrakóði used by the central ERP system Example: FJR, HMS, THSK	Organisation ID	Mandatory
Owner	E-mail john.doe@government.is	Resource or application owner	Mandatory
ReviewedDate	Text in date format *2023-10-20*	Date, which tells on when the last review has been done for the resource	Mandatory
Criticality	Business Critical Critical Non-Critical	Business criticality of the Resource or application	Optional
SLA	Gold Silver Bronze	Service Level Agreement for the workload / application	Optional
CostCenter	Number (Viðfang) as specified in the Orri ERP system.	Cost center / project responsible of the costs related to the Resource or application	Optional
OpsTeam	Text Umbra	Team or partner operating the Resource or application	Optional
EndDate	Text in date format 2024-01-22	The assumed end date for the use of the Resource.	Optional
Requester	E-mail john.doe@government.is	The person who has requested the Resource	Optional

Note! The format of the tag and the value is important. Use the precise letter case (upper or lower) format as given above.

5.5. Resource removals

Removing unneeded resources must be ensured to enable cost savings. However, continuity must also be ensured – when resources are removed, accidents may occur. Azure offers certain protections – which are defined in this policy area – for these kinds of situations.

The policies related to Resource Removals are stated in the following table.

SCOPE	POLICY
Generic principle	When Resources are removed, all the related Resources – that are no longer being used – must be removed as well. Examples of such Resources include: Resource Groups, public IP addresses and storage services.
Resource Locks	Resource Locks are used for Resources that cannot be removed without a separate approval. This lowers the risk of large-scale incidents caused by human errors. More of Resource Locks in chapter *5.7.3 Resource Locks*.
Removal of productional environments	Prior to removing productional Resources the Resources must be shut down, stopped or otherwise sealed from the environment for seven (7) days. This ensures that the Resources are not being used for some other use. Use *EndDate* (see: *5.4 Tagging)* to tag the period, when the Resource may be removed.

5.6. IAM practices

Everything in Azure revolves around Azure AD. That is why it is also important to plan and define IAM when it comes to setting up the usage policies.

There are two sides to the coin:

1. How users are created
2. How access is granted to the users.

The first point is more related to how Active Directory itself is managed, hence this Governance Framework focuses more on how access is granted to the users (i.e. *Role-Based Access Control*).

The policies related to IAM practices are stated in the following table.

SCOPE	POLICY
Administrative accounts	Administrative accounts are separated from “office accounts”
Location of Administrative accounts and groups	Administrative accounts can be synced accounts (from on-premise Active Directory). Administrative groups are cloud-only.
Granting Rights	Rights are granted to groups, not individual users (with the exception of root management group)

Granting Rights	Only individual users are granted owner rights to the Root Management Groups. There should be at least two (2), but preferably three (3) users with owner rights to Root Management Group. Groups are not used, so that a user with group management rights in Azure AD cannot grant themselves rights for the Root Management Group.
Granting Rights	Least privilege must be applied. Grant only the rights needed. Remember also inheritance – if you grant access to a higher level in the management structure, it will fall to all the resources directly beneath it
Azure AD B2B	Azure AD B2B for external users is not allowed for administrative purposes.
Remote management of Virtual Machines	Use Azure Bastion for remote management of Virtual Machines.

5.7. Continuity

The **Strategic Cloud Policies** state the following:

- *Strategic cloud policy 4.3: The **continuity and availability requirements** of the processes are achieved by **developing a cloud native high availability architecture together with SLAs in the cloud contracts**.*
- *Strategic cloud policy 5.3: **The data in cloud services and platforms must always be easily transferable to other platforms or systems**. **Continuity must be ensured in all cases based on the business continuity needs**.*
- *Strategic cloud policy 6.2: **Constantly monitor your services**. Create technical capabilities to provide **real-time insight on your environment's health**.*

While continuity is a larger subject altogether – ranging from day-to-day operations into business continuity in disaster scenarios – in the Governance Framework we cover the following four subjects:

1. Monitoring: how applications, services and resources are being monitored
2. Resource Locking: how accidental or malicious removal of resources is prevented
3. High availability: how redundancy is considered when building up solutions
4. Backup and recovery: how to ensure recovery of data and services in case of faults or accidental/malicious removals.

The policies related to Continuity are stated in the following chapters.

5.7.1. To be considered: business continuity in Azure

Business continuity, i.e. the continuity of the applications and solutions created for "business purposes" (in this case an example could be a patient registry used by the National Hospital) typically have recovery time objective

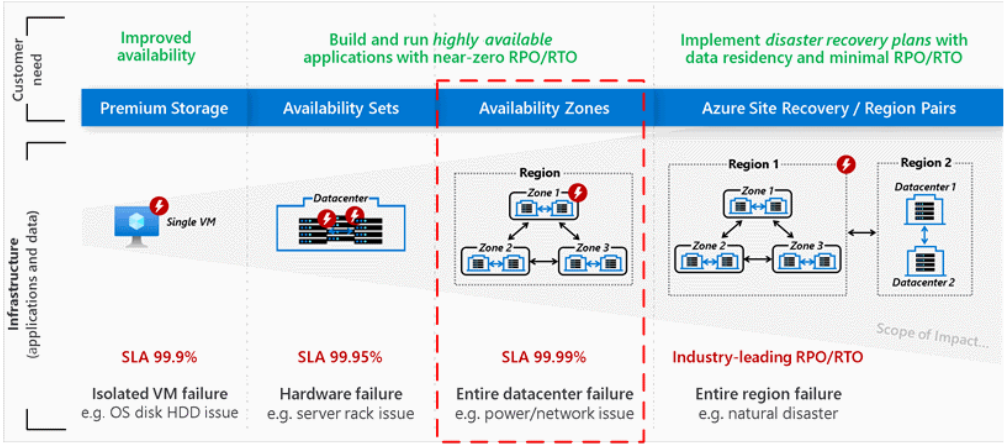
(*RTO*) and recovery point objective (*RPO*) requirements. These requirements work as a base for designing continuity solutions, which may include:

- High availability – e.g. clustering the environment, so that it is not dependent on a single point of failure
- Disaster Recovery – both a technical solution to return the system and it's data to use and the surrounding process and guides on how the system is returned to use. Technologies may include such as:
  - Backups – recovering workloads, applications and data from backups
  - Cold site – recovering the system using a secondary site and backups
  - Replication – recovering the system using a passive, nearly identical and up-to-date environment.

***RTO** states the timeframe in which the system must be functional. For example, an RTO of 24 hours would state that the system is operational latest 24 hours from failure.*

***RPO** states the accepted loss of data in time. As an example, RTO of 4 hours would state that losing the last 4 hours of data from failure would be acceptable..*

When it comes to Azure (and cloud services in general), it is vital to understand that the cloud service provider does not ensure continuity for business applications and data. The customer needs to plan the business continuity according to their requirements. See the following picture (source*:* *https://learn.microsoft.com/en-us/azure/architecture/high-availability/building-solutions-for-high-availability*) that describes the SLA guarantees Microsoft promises to different High Availability / Disaster Recovery scenarios.



5.7.2. Monitoring

SCOPE	POLICY
Generic policies	All productional environments and their Resources are monitored.

	Each Institution is accountable for organizing the monitoring capabilities. Tenant Operators may offer this service to the Institutions in each Tenant.
Location of logs used by Azure Monitor	Azure Monitor related logs are stored either in a centralized Log Analytics Workspace or in a Log Analytics Workspace by Subscription. The decision is made by the Tenant Operator by Azure Tenant.
Application monitoring	Each system owner is responsible of their applications' monitoring capabilities. Azure Monitor Application Insights may be utilized for application monitoring when applicable.
Connection to Incident Management process	Connection to Incident Management process and possible ITSM tooling is done on a later phase, not currently available.

5.7.3. Resource Locks

SCOPE	POLICY
Generic policies	All productional Resources must be – by default – protected with Resource Locks.
Responsibilities	Each system owner is responsible of Resource Locks in their environment.
How to lock	Productional Resources must be locked with the "CanNotDelete" mechanism.

5.7.4. High Availability

SCOPE	POLICY
Redundancy (multiple availability zones)	Each system owner can decide of the implementation of redundancy according to the business requirements. (see: *5.7.1 To be considered: business continuity in* Azure)
Geographical distribution	Each system owner can decide of the implementation of geographical distribution according to business requirements. The location restrictions stated in *5.2 Region* must be considered.

5.7.5. Backup and Recovery

Each system owner is responsible of defining the backup and recovery mechanisms based on RPO/RTO needs and a risk-based evaluation. The following table describes the policies and procedures if there are no specific requirements for the system.

SCOPE	POLICY
Generic policies	For society-critical applications a 3rd party backup tool (currently: Veeam) must be considered to enable backups to a separate location/environment outside of Azure. The native service – Azure Backup – is used if no other solution is applicable or available. Default backup policies (see below table) are used, but application specific deviations may be defined, if there is a business need.
Backup lifecycle management	Azure Backup service manages the lifecycle of backups performed by it. Each system owner is responsible of the lifecycle management of manually performed backups.
Tooling	3rd party backup tool is used for the backup of society-critical **Virtual Machines and databases running on virtual machines.** Azure Backup and SQL Server Backup is used for other **Virtual Machines and databases running on virtual machines**. Built-in backup functionality is used for **PaaS-databases** (Azure SQL Managed Instance and Azure SQL Database).
Soft delete for backups	Soft delete functionality ensures that backup data is not deleted by accident or in malicious purposes. Soft delete is enabled by default and must not be removed.

Default backup policies are defined in the following table. These may be changed according to business needs.

SCOPE	POLICY
Productional environments	Daily backups: retention time 7 days Weekly backups: retention time 4 weeks Monthly backups: retention time 12 months Application-specific deviations may be defined.
Test and quality assurance environments	Daily backups: retention time 7 days Weekly and monthly backups: no retention requirements Application-specific deviations may be defined.
Development environments	Daily, weekly and monthly backups: no retention requirements Application-specific deviations may be defined.

5.7.6. Data continuity

SCOPE	POLICY
Soft delete	Soft delete must be enabled for productional blobs, storage containers and file shares.
Versioning	Versioning can be enabled for blobs and storage containers, if seen fit. System owner is responsible for defining and enabling this feature. Versioning is required for data classification levels 3 and 4 (see: *Data Security Classification of the Icelandic government, 05/2023*)

5.8. Networking

Networks are a major building block in the public cloud as well. Through them you can segment application workloads and add security layers and enable access to end-users.

The policies related to Networking are stated in the following table.

SCOPE	POLICY
Connections to the on-premise networks	Connections to the on-premise networks is done through a VPN connectivity over the Internet when necessary. ExpressRoute may be used in the future, but not currently implemented.
Network topology	Currently, the network architecture is implemented as individual virtual networks. Target setup per tenant would be to have a hub-and-spoke network topology, but it is not currently implemented. In the hub-and-spoke topology the virtual networks (vnet) are connected to each other through a centralized virtual network and a router/firewall located there.

Name resolution	DNS service located in each institutes Active Directory is used. The DNS-services will be connected to the Azure Private DNS service if deemed necessary.
IP addressing	Tenant Operator and the Institutions are responsible of the IP network allocations for each system/need.
Virtual network connectivity	Virtual networks are connected to each other through Network Peering when needed, unless a hub-and-spoke topology is in place. If a hub-and-spoke topology is in place, all communications must flow through the hub network.
Use of PaaS services	PaaS services are primarily used through Service Endpoints (if only used inside Azure) or Private Endpoints (if used from on-premises as well).
Azure Bastion	Deploy a centralized Azure Bastion per Azure Tenant (or Instutition when applicable) to enable remote management for Virtual Machines in a cost-effective and secure way.

Policies specific to network security are stated in the following table.

SCOPE	POLICY
Generic policies	All traffic inbound and outbound is denied by default. Access policies / firewall openings must be requested by each system owner through the Institution/Tenant Operator specific channels. Unsecured HTTP must not be used for publishing services externally. All external websites and other HTTP-based communications must use HTTPS.
Use of Network Security Groups	Network Security Groups are used on both subnet and network interface levels. Generic policies are defined on a subnet level, which can be specified on the interface level.
Publication of applications	Applications are published by default using services such as Azure Load Balancer and Azure Application Gateway.
Application Security Groups	When possible, Application Security Groups shall be utilized for protection and ease of management of multi-layer application environments (such as application workloads and database environments).
Virtual networks	Create a virtual network (vnet) per Subscription. Use subnets and network security groups to segment applications and workloads from each other in a virtual network. If there is a need to segment on a virtual network level, additional virtual networks can be created in a Subscription.
Use segmentation on subnet level	Segment the virtual networks into subnets as needed. As an example, segment shared database resources to a

	separate subnet and each application to their own subnets.
Enable Azure Web Application Firewall	Use this with HTTPS traffic
Enforce HTTPS-only communication	Ensures the user-to-app internal traffic is encrypted.
Use Cloudflare for DDoS protection of critical workloads	Cloudflare is preferred for Distributed Denial of Service attack protection over Azure native service (Azure DDoS Protection)

5.9. Security

Security is also a wide area, but in this Governance Framework the following six key risk areas addressed by Zero Trust Framework are defined:

1. **Identity:** Automate risk detection and remediation. Secure access to resources with strong authentication
2. **Endpoints:** Defend larger attack surface created by the growing number of endpoints using integrated approach to management
3. **Data:** Classify, label and protect data across cloud and on-premises environments to help prevent inappropriate sharing and reduce insider risks
4. **Apps:** Institutions must find the right balance of providing access while maintaining control to protect critical data accessed via applications and APIs.
5. **Infrastructure:** Protect hybrid infrastructure, including on-premises and cloud environments, with more efficient and automated management
6. **Network:** Reduce perimeter-based security vulnerabilities. Instead of believing everything behind corporate firewall is safe, Zero Trust strategy assumes breaches are inevitable.

The following sections cover the Identity and Infrastructure, while Network security is covered in chapter *5.8 Networking*. Endpoints, data and apps are not part of this Governance Framework.

5.9.1. Identity

POLICY	DESCRIPTION
Roll out Azure AD MFA	Multi-Factor Authentication helps safeguard access to data and applications, providing another layer of security by using a second form of authentication. Organizations can enable multifactor authentication (MFA) with Conditional Access to make the solution fit their specific needs.
Block legacy authentication	One of the most common attack vectors for malicious actors is to use stolen/replayed credentials against legacy protocols.
Use Privileged Identity Management	Currently not implemented to the Azure Tenants!

	Provides a time-based and approval-based role activation to mitigate the risks of misused access permissions to important resources

5.9.2. Infrastructure

POLICY	DESCRIPTION
Enable Microsoft Defender for Cloud with Standard Tier	With this you can incorporate a set of baseline controls through Azure Policy and monitor the compliance of specific workloads
Deploy Microsoft Defender for Servers and Containers	Deploy Defender for Servers and Defender for Containers to productional workloads.
Govern how resources are deployed	You can e.g., only grant contributor access for DevOps pipelines that uses predefine templates
Use policy to enable logging to a central log analytics workspace	You can enforce workloads to log automatically to specific Log Analytics Workspace
Use policy to enable diagnostic logs for every resource	You can enforce workloads to collect diagnostic metrics to specific Log Analytics Workspace

5.10. DevOps

The **Strategic Cloud Policies** state the following:

- Strategic cloud policy 5.2: Leverage a wide range of the technical capabilities of the chosen cloud environment. **Use native automation tools and value add services.**
- Strategic cloud policy 5.4: Utilize the elasticity of cloud services **using iterative and experimentative development model**. Publish and test often, start small and expand according to growing needs.
- Strategic cloud policy 6.1: **Fully automize your services**. Leverage automation tools to **scale your services based on demand and automate changes to your environment**.

DevOps enables development, IT operations, quality engineering, and security to coordinate and collaborate to produce better, more reliable products. With DevOps culture along with DevOps practices and tools, teams gain the ability to increase confidence in the applications they build and achieve business goals faster.

The policies related to DevOps are stated in the following table.

POLICY	DESCRIPTION
Use Azure AD Groups	Use AAD Groups to handle permissions if possible.
Block external guest access	Don't allow invitations to be sent to any domain. For external consultants and partners an identity must be created for the Azure Tenant in question.
Limit access to projects and repos	Reduce the risk of leaking sensitive information and deploying insecure code
Use Approval Gates	You can add members to Approval Gates so their approval is needed when e.g., deploying to production
Secure secrets	Use the combination of Azure DevOps Library secret variables and Azure KeyVault to secure secrets
Use code reviewing	Require at least one reviewer outside of the original requester
Use PR's (Pull Request)	Deny that code can be directly merged to production branch
Disallow completion of a PR from the requester	Don't allow the original pull requester to approve their own PR's
Always use different credentials for dev, test and production environments	Make environment specific credentials
Use YAML pipelines	Manage pipeline definition with YAML. It provides version control which the "UI pipeline" doesn't

Don't store secrets in pipeline variables	Avoid using hard coded secrets straight from the YAML. Use Library Secret Variables
Enable Audit logging	Enable logging for the Azure DevOps and if possible sent the logs to Log Analytics Workspace which is linked to Microsoft Sentinel

6. Enforcement of the policies

When establishing Institution or Tenant-wide governance strategies there are different kind of ways to achieve that:

- Baseline recommendations
- Policy compliance monitoring
- (Azure) Policy enforcement
- Cross-Organization enforcement
- Automated enforcement.

It is to be noted and understood, that the purpose of a policy enforcement is not to make the creation of new services hard but ensure the compliancy of the environment.

The following table describes the minimum policies to be set to each Tenant. Each Tenant Operator and individual Institution may add policies according to their needs.

POLICY	DESCRIPTION	Enforced
Allowed locations	This policy enables you to restrict the locations the Institutions can specify when deploying resources (see: *5.2 Region*). Use to enforce your geo-compliance requirements. Excludes resource groups, Microsoft.AzureActiveDirectory/b2cDirectories, and resources that use the 'global' region.	Yes
Allowed locations for resource groups	This policy enables you to restrict the locations the Institutions can create resource groups in (see: *5.2 Region*). Use to enforce your geo-compliance requirements.	Yes
Allowed resource types	This policy enables you to specify the resource types that your organization can deploy. Only resource types that support 'tags' and 'location' will be affected by this policy. To restrict all resources please duplicate this policy and change the 'mode' to 'All'.	Yes
Not allowed resource types	Restrict which resource types can be deployed in your environment. Limiting resource types can reduce the complexity and attack surface of your environment while also helping to manage costs. Compliance results are only shown for non-compliant resources.	Yes
Audit resource location matches resource groups location	Audit that the resource location matches its resource group location	Audit
Audit usage of custom RBAC rules	Audit built-in roles such as 'Owner, Contributer, Reader' instead of custom RBAC roles, which are error prone. Using custom roles is treated as an exception and requires a rigorous review and threat modeling	Audit and Disabled

Start/Stop VMs during off-hours overview	The Start/Stop VMs during off-hours feature start or stops enabled Azure VMs.	Yes
Require a tag and its value on resource groups	Enforces a required tag and its value on resource groups. See *5.4 Tagging*.	Yes
Require a tag and its value on resources	Enforces a required tag and its value. Does not apply to resource groups. See *5.4 Tagging*.	Yes
Add a tag to subscriptions	Adds the specified tag and value to subscriptions via a remediation task. If the tag exists with a different value it will not be changed. See *5.4 Tagging*.	Yes
Add a tag to resources	Adds the specified tag and value when any resource missing this tag is created or updated. See *5.4 Tagging*.	Yes
Inherit a tag from the subscription if missing	Adds the specified tag with its value from the containing subscription when any resource missing this tag is created or updated. Existing resources can be remediated by triggering a remediation task. If the tag exists with a different value it will not be changed. See *5.4 Tagging*.	Yes
Inherit a tag from the resource group if missing	Adds the specified tag with its value from the parent resource group when any resource missing this tag is created or updated. Existing resources can be remediated by triggering a remediation task. If the tag exists with a different value it will not be changed. See *5.4 Tagging*.	Yes
Enforce Resoure Locks	Prevent users from deleting or modifying Azure resources. Keep in mind that if you don't let modify resources they usually can not be updated via DevOps pipelines. See: *5.7.3 Resource Locks*.	Yes
Azure Backup should be enabled for Virtual Machines	Enforce backup for all virtual machines by backing them up to an existing central recovery services vault in the same location and subscription as the virtual machine.	Yes
Deploy default Microsoft IaasAntimalware extension for Windows	This policy deploys a Microsoft IaaSAntimalware extension with a default configuration when a VM is not configured with the antimalware extension.	Yes
Deploy Diagnostic Settings for every resource that supports it	Collect all the Diagnostic Settings in a centralized manner to a one specific Log Analytics Workspace	Yes
Configure Azure Activity logs to stream to specified Log Analytics workspace	Deploys the diagnostic settings for Azure Activity to stream subscriptions audit logs to a Log Analytics workspace to monitor subscription-level events	Yes
Configure Log Analytics extension to be enabled on Windows virtual machine	Deploys the Log Analytics extension to a Windows virtual machine	Yes
Configure Log Analytics extension to be enabled on Linux virtual machine	Deploys the Log Analytics extension to a Linux virtual machine	Yes
Configure Windows virtual machine to run Azure Monitor Agent	Deploys AMA to Windows virtual machine	Yes
Configure Linux virtual machine to run Azure Monitor Agent	Deploys AMA to Linux virtual machine	Yes
Configure Microsoft Defender for servers to be enabled	Enables defender for servers to monitor the security posture of virtual machine	Yes

Configure Microsoft Defender for containers to be enabled	Enables defender for containers to monitor the security posture of containers	Yes
Deny inbound RDP from the internet	If you try to create a new NSG rule which allows inbound port 3389 from the internet, it is denied by policy	Yes
Audit VMs without disaster recovery configured	Audit virtual machines which do not have disaster recovery configured.	Audit
Audit VMs that do not use managed disks	This policy audits VMs that do not use managed disks	Audit