Governance

Governance, within a company, are the leaders/processes that set the rules.

Who se t these policies: Board of directors, CEO, Director of Development, can also be a formal group like IT Security Committee or Architecture Review

Types of Rules:

- All servers must be running software within Microsoft Extended Support guidelines
- Backup standards – All Servers must be backed up every 24 hours at a minimum
- Network standards – Firewalls must block all inbound ports from the internet except 443
- Only operations support can reboot a production server (certain people have control on certain tasks)

Then we have to make sure the platform (Azure) to audit or enforce the rules. That is the concept of Governance and Compliance in Microsoft Azure.

To carry out these, we have (software):

- Azure Blueprints (now retired) -> (replaced with) Template Specs
- Deployment Stacks
- **Azure Policy** (predefine rules, we can also define rules (run most recent Windows, do not go beyond certain SQL version, etc.). This could be applied to certain resources or resource group(s). Examples of Policies:
    - Require SQL Server 12.0
    - Allowed deployment locations (e.g. only in EU region)
    - Not allowed resource types (no web apps)
    - ....
- Resource Locks (lock production resources so that they cannot be deleted accidentally.)
- Microsoft Purview (data governance)
- RBAC (role-based access control)

Resource Locks

They give ability to restrict the modification or deletion of resources.

Also, prevents accidental (or malicious) deletion of critical resources. So, you would not put resource locks in development/testing resources, only in production scenarios.

Many people may need access to a resource (like to restart a VM), but deleting it has severe consequences.

Types of Resource Locks (in Azure):

- Read Only: Prevent any configuration changes (e.g. size) to the resource. Even the owner (who created the resource) is preventing from deleting it.
- Can Not Delete: Allows configuration changes but can not delete it.

At what level we can implement these locks (Scope)?

- Resource level
- Resource group level
- Subscription level

Note that resource locks are a weak form of security (roles-based access are important and resource locks mainly stop accidents).

Microsoft Purview – Data Governance tool

This is a centralized dashboard for all data governance issues. There are a lot of purviews:

- Auditing
- Communication Compliance
- Information Protection
- Data Loss prevention
- ...

Communication Compliance

- Sensitive or confidential information
- Harassing or threatening language
- Sharing of adult content
- ...

Then, we can check who violated which policies and so on.

Information Protection

- know your data: what sensitive information is stored where (e.g. credit card information)
- Protect your data: sensitivity labels (e.g. secret, top secret, eyes only), encryption
- Prevent data loss: browser extensions, pop-up tips, block sharing, hide from chat

Insider Risk Management

Insiders - People work in the company and have access to the system.

We do not want potential malicious or inadvertent actions from insiders.

- IP theft
- Data leakage
- Security violations

Since it may not be ethical / make employees work freely, when they are been watch all the time. Thus, certain actions can be taken (examples):

- Data theft by departing employees
- Risky browser usage (flag the employee)
- Request not to disable important security features. Monitor installing malware
- Check on unusual export of patient data