# Secure & govern IT operations in local gov

## Local operations are no longer local – a new reality

For many years, local government have seen their IT operations as something that takes place locally. The servers are located in their own data centers, the operating staff has their hands on the equipment, and the IT department experiences a sense of full control. It is a culture that is built on experience, professionalism and pride.

But quietly – almost invisibly – the architecture has changed. Today, the local operations are interwoven with Microsoft's cloud services, especially Azure. Not because the organization has actively chosen a cloud strategy, but because Microsoft's technologies **are gradually moving control functions out of the house**.

This means that many local government organizations actually run **hybrid operations**, without having a hybrid governance model.

## Azure as a foundation—even when servers are on-premises

The most important realization is this:

**The on-premises datacenter relies on Azure, even if workloads are physically located at the It department.**

Most organizations today use:

- Microsoft Entra ID (formerly Azure AD)
- Intune for PC control
- Microsoft Defender for threat protection
- Azure Monitor and logging
- M365 for daily operations and access management

These services are not located locally. They reside in Azure – and they increasingly determine how the local part works.

### Identity – the heart of operations and access

When an employee logs in to a PC, an administrative system or Teams, it is Azure that decides:

- Who the person is
- What rights they have.
- Which rules are enforced.
- Whether the login is valid at all

A change in Azure can therefore stop local operations – without the organization itself having touched anything.

# Secure & govern IT operations in local gov

### Security – protection is in the cloud

Modern security is built on cloud intelligence. Defender gets its rules, signatures, threat profiles, and responses directly from Azure. If this connection or control fails, security is breached – even locally.

### PC and device management—Intune takes over

IT department often have both SCCM and Intune, but Intune is now Microsoft's primary engine. Policies, updates, and security rules are deployed from Azure. A change in Intune will immediately hit PCs at city halls, schools, and institutions.

### Monitoring and logging

The IT department's ability to detect errors, breaches and abuse is increasingly dependent on Azure Monitor, sign-in logs and M365 audit logs. This means that the "operational overview" is no longer on-premises – it is cloud-managed.

## Dependency without governance – the biggest hidden risk

Local government IT have become dependent on Azure, but many do not actively manage Azure.

The result is a governance challenge that affects three key areas:

1) **Operational risks**
   Experience errors that seem random. Often, these look like local failures – but the reason lies in the cloud's control plan.

2) **Security risks**
   Lack of governance creates gaps with broad privileges, external vendors with unintended access, expired tokens, open service accounts, policies that are not updated automatically.

This is where many organizations become vulnerable to ransomware attacks.

3) **Compliance and NIS2**
   Public organizations must document how access is granted, security is enforced, changes are managed, operations are kept secure and updated, and how to detect and respond to breaches.

   If half of the operations are in Azure – but governance does not follow – a large part of the documentation is missing.

**This is precisely the reason why many public organizations face challenges with NIS2.**

# Secure & govern IT operations in local gov

## Why the problem is underestimated

There are three reasons:

1) **Local**
IT departments are used to physical operations and a high level of control. Therefore, it still feels "local", even when the control is out in the cloud.

2) **Azure's influence is invisible**
A change in Conditional Access doesn't feel like the cloud. It feels like a local login error.

3) **Resources are under pressure**
An IT department of 8–12 people cannot keep up with Microsoft's pace of change without automation. Therefore, governance becomes an area "you take when you get time" – and that time will never come.

## It's only getting more important
## Azure is the control plane of the future

Microsoft's strategy is clear:

- Security comes first in the cloud
- New features land in the cloud, not on-premises
- On-prem governance is built on top of Azure Arc
- Hybrid operation becomes standard
- NIS2 pushes the requirements further

Therefore, the organizations can no longer run local IT without also having control of Azure.

It's not a choice – it's a technical reality.

## What governance should be in an organizational context

A realistic governance model for organizations must be:

- **automatically** (because manpower doesn't exist)
- **standardized** (because the organization does not have to invent its own rules)
- **continuously updated** (because Microsoft changes hundreds of things annually)
- **documented** (for NIS2 and audit)
- **simple to be responsible for** (regardless of internal roles or replacement)

In other words: the organization should not be an expert in Azure.

It must have a system that ensures that operations remain correct – without extra work.

# Secure & govern IT operations in local gov

## MyPlatform as a solution layer

MyPlatform was developed based on experiences from:

- **City of Copenhagen**
- **Frederiksberg City**
- **HOFOR**
- as well as other highly regulated organizations

All local government organizations face the same challenge:

The risk does not lie in the cloud – it lies in the lack of governance between cloud and on-prem.

Today, operation is inevitably hybrid. Systems, networks, and data reside both on-premises and in Azure.

Therefore, security, compliance and governance must be built right from the start – across the entire infrastructure, not just the on-premises data center and not just in the cloud.

**MyPlatform** is built just for that. Not as a "cloud project", but as a governance and operating platform that ties the hybrid environment together:

- Automates Microsoft's ongoing changes
- Keeping Policies, Security & Compliance Evergreen
- Ensures documentation ready for auditing
- Provides stable, consistent operation in both cloud and on-prem
- Eliminates the need for manual corrections and cumbersome consulting processes
- Respects the existing operating model

The point is not to move everything to the cloud - the point is to manage the hybrid environment the organization already has - correctly, securely and continuously.

# Secure & govern IT operations in local gov

## Conclusion: Local government can operate on-premises, but not without Azure governance

The organizations facing a new hybrid reality. The servers are still on-premises, but the control lies in Azure. Therefore, governance must be changed, not operations.

The local government organizations can achieve:

- Stable operation
- Fewer errors
- Better security
- documentation for NIS2
- Less vulnerability when replacing employees

... if they accept that the future of on-premises operations requires a governance model that matches Microsoft's control plan.

**Governance is not cloud – governance is operation.**