us signal

# 5 Cloud Migration Considerations for Government

**For government entities the cloud offers a way to reduce costs, meet security and regulatory requirements, and ensure high availability for their critical systems. However, government IT departments face some unique challenges when migrating to the cloud because of regulatory, security and stringent application requirements. If you're part of a government IT team struggling with these challenges, here's a checklist of considerations to help relieve migration headaches:**

## public, private or hybrid

Selecting the right infrastructure for your cloud deployment is critical to your success. An in-depth evaluation of your current applications and infrastructure is needed to determine the right cloud choices for your organization.

**Evaluate the following needs of each application to ensure cloud success:**

- ✓ **Performance.**
- ✓ **Security.**
- ✓ **Data needs.**

## high availabilty

Government operations require 24/7/365 access to data, desktops, applications and communications from anywhere on any device.

**Address these concerns by:**

- ✓ **Demanding strong SLAs.**
- ✓ **Defining application specific performance needs upfront.**

## education

Assess the skill set of your municipality's IT organization and understand if they have the right training to manage your cloud infrastructure.

**Ensure your employees are:**

- ✓ **Well versed in operating and managing your cloud environment.**
- ✓ **Handling problems as they arise.**

## security and compliance

For any government agency, ensuring appropriate security of your applications and data is vital. Develop a strategic plan that identifies where the risks lie and address how to protect sensitive data.

**Security policies and protocols should be set in place that addresses:**

- ✓ **Physical security.**
- ✓ **Cloud security.**
- ✓ **Encryption.**
- ✓ **Compliance mandates, (PCI-DSS, HIPAA)**

## disaster recovery

One aspect of IT infrastructure that often gets neglected is application resiliency and disaster recovery.

**Your cloud provider should:**

- ✓ **Explain its own plan for disaster recovery, and provide you with a clearly documented service level agreement (SLA) to help you to plan yours.**
- ✓ **Have facilities in multiple regions to ensure a degree of safety in the event of natural disasters or terrorist action.**