Browne Jacobson

Reaching cloud nine? Public procurement for cloud-based services

20 January 2023

Alex Holbrook examines how to navigate procurement for cloud-based services.

In 2013, the government launched the 'Cloud First' policy for all technology decisions. The Cloud First policy is a strategy that will encourage local authorities to consider cloud-based solutions as a first port of call when looking to new technologies or services. This policy is becoming more popular among local authorities as it offers a number of benefits such as cost savings, scalability, and flexibility.

However, it is essential that public sector conduct thorough due diligence to ensure that they are selecting the right cloud provider to meet their specific needs and requirements. Local authorities should also evaluate the provider's pricing and billing structure, as well as any additional costs or fees that may be associated with the service. The key factors to consider during due diligence are explored as follows:

Cost savings

By using cloud-based services, local authorities can reduce their IT costs as they will not be required to invest in expensive hardware and software. Furthermore, cloud providers often offer pay-as-you-go pricing models, which can help local authorities manage their budgets more effectively.

Scalability

Cloud-based services can easily be scaled up or down as required, making it easy for local authorities to adjust their IT resources to meet changing demands. Scalability in cloud computing can be referred to in one of two ways:

- vertical scaling: this is when more power is added to an existing instance (i.e. more memory/RAM, faster storage, or more powerful processors (CPU)), and
- horizontal scaling: this is when more servers are added to spread the load across multiple machines. This comes with added complexity as multiple servers will now require updates, security, and monitoring.

Flexibility

Cloud-based services allow local authorities to access their data and applications from any location with an internet connection; enabling remote working and collaboration.

Security

When procuring cloud solutions, it is important to first understand the intended use of the cloud service and the data that will be stored and processed in it. Local authorities will then be able to choose a cloud provider that meets its security needs.

Many cloud providers have robust security measures in place which can help protect local authorities' data against breaches and cyber-attacks. Examples of added layers of security on cloud-based solutions include encryption and multi-factor authentication. Additionally, users wishing to access the data will need to have a digital key. Cloud-based data is therefore generally more secure than data stored on computers connected to the internet.

Dependence on internet connectivity

Cloud-based services rely on a stable internet connection which can be a problem for local authorities in remote areas and can lead to unpredicted periods of downtime (i.e. time during which the cloud services would be out of action or unavailable for use). Downtime is often one of the biggest risks of using cloud-based services due to the fact that it is internet based.

One of the best ways a local authority can minimise the risks of downtime in a cloud environment is to ensure that the service levels are guaranteed at a 99.9% uptime or better. To put this into context, a 0.1% downtime on a 24/7 365-day service equates to 8 hours 45 minutes 36 seconds downtime per year.

Cloud provider lock-in

Local authorities may become locked into a specific cloud provider and find that it is difficult to switch to a different provider in the future, which can limit their flexibility and increase costs. Cloud provider lock-in can come about in the following ways:

1. The database on the cloud starts out small but, with increasing volumes of data, becomes too data-heavy to migrate; therefore locking local authorities into their cloud service provider.
2. A cloud-based application is linked too tightly to the cloud platform. This means that the local authority would have to rebuild an entirely fresh application upon switching to a different provider.
3. The cloud service provider requires an advance notice (e.g. 30 days) for termination. Although this is not as strict of a lock-in, it still means that local authorities would be unable to switch over immediately.

Compliance and regulatory

Local authorities may have difficulty ensuring compliance with certain regulations and standards when using cloud-based services, as they may not have full visibility into the provider's security and compliance practices.

Ensuring that cloud-based service is legally compliant will involve:

- in line with UK GDPR:
  - knowing where cloud data is stored and processed,
  - ensuring that personal data is handled distinctly from other data,
  - strictly controlling the collection of special category data (e.g. ethnicity or sexual orientation), and
  - ensuring that data can be quickly accessed and deleted as necessary.
- applying a risk management framework for the data, and
- ensuring that ISO standards, certifications and attestations are put in place. These include:
  - ISO/IEC 27001: Information Security Management,
  - ISO 9001: Quality Management Systems, and
  - local authorities may also adopt a risk management framework specific to cloud computing, such as ISO/IEC 27017: Cloud Specific Controls, or
  - CSA Security Trust Assurance and Risk attestation.

By procuring a cloud-based provider with the above accreditations, the local authorities can engage with the provider with the peace of mind that they are compliant with ISO standards.

This article was first published by Local Government Lawyer on 20 January 2023.

Contact

Henrietta Scott

Head of Marketing

PRTeam@brownejacobson.com

+44 (0)330 045 2299

Related expertise

Services

Commercial and outsourcing for health

Digital and sourcing

Information law

Local government procurement

Public contracts, projects and funding

Public procurement