AdviSec Ltd

LOCAL AUTHORITIES

Background

In this period of austerity facing the UK, local authorities are under severe pressure to deliver significant costs savings, and these pressures are likely to continue for some years to come.

Sharing ICT infrastructure, staff with specialist skills, and premises offers the opportunity (potentially) for significant costs savings, for example why should each Council have its own HR and Finance application systems, connection to the Internet, or standby data centre?

The 'Public Sector Network' (PSN) has been developed by Central Government as a mean of affording organisations the opportunity of 'sharing' ICT infrastructure. However Local Authorities are different from central Government departments, and even within the sector there are variations (e.g. County Council versus the Town or Borough council, rural versus urban) and as such the 'benefits' of adopting the PSN concept, either as a Customer or 'Direct Network Service Provider' (DNSP) need careful consideration.

Local Government consists of a number of bodies, many of which perform an important function involving 'sensitive' information, which needs to be stored, processed and/or transmitted. It should be noted that some information is particularly 'sensitive' and needs to be handled at a higher-level than PROTECT, e.g. RESTRICTED. Local Government requires facilities to exchange such information both within the organisation and between itself and other organisations, for example:

- Social care, YOTS, Schools (including those under LEA control and academies), LEA ('internal' information exchange)
- Police, Health, Charities / Voluntary sector, Fire, Central Government ('external' information exchange)

The AVAILABILITY of application services and associated information is as important as CONFIDENTIAILITY and INTEGRITY.

Facilities

Local Government currently makes very little use of shared infrastructure operated by other organisations, with the exception of:

- Communication circuits and networks provided by the commercial communication providers
- National networks, such as the GCSx or GSx (all Councils), N3 (most Councils), CJK / PNN3 (a few Councils) which are used to exchange information with particular organisations.

Some Councils 'lead' on the provision of services across their region, for example museums, traffic signals, and provide the IT infrastructure, including 'dedicated' communication networks, to support these operations.

Other forthcoming developments that need to be addressed include:

- Transmission of CCTV across converged networks; note many Councils already have a converged data and telephony network
- Opportunities for using WiMax
- Provision of WiFi and Internet services in libraries, business parks
- Provision of 'open networks' that may be used by telecoms providers
- More academies, with their greater independence from the Local authorities, and the increased risk of bespoke IT solutions which arises.
- The requirement for resilience and disaster recovery with regard to the Civil Contingencies Act, and including in particular a standby data centre.
- Co-location of organisations
- Agile working and remote access technologies, e.g. 3G/4G, xDSL, Public WiFi

It should also be noted that the national networks provided by Government and the 'major' telecoms providers will be PSN compliant in the 'future' which will have an implication for Local Government and the need to comply with the PSN Code of Connection.

How can we help?

Our consultants can:

1. Meet with Councils, business leaders, the Emergency services and Others to understand the opportunities for sharing premises, IT and communications infrastructure, and even staff performing key IT and security-related functions.

2. Highlight the opportunities for Councils to act as a DNSP taking account of the OGC Green Book guidelines for preparing an Outline Business Case:

    - *Strategic case* – describes the project rationale, objectives, benefits, and the case for change
    - *Economic case* – appraises different options under consideration including a SWOT analysis

- *Commercial case* – explores funding sources, asset ownership, procurement strategy, key contractual issues and TUPE issues
- *Financial case* – details cost modelling outputs of options under consideration exploring different charging/apportionment models and shows a comparison of all the options
- *Management case* – describes management responsibilities, governance and reporting, delivery plan, project management methodology, change management, stakeholder management, contract management, risk management and benefit realisation plan and benefit register.

The 'drivers' underpinning the PSN are seemingly obvious, however there are constraints which our consultants are fully aware of, and which need to be assessed when putting forward recommendations for organisations to take-on the role of a DNSP or 'Customer', for example:

- The resources required to comply with the PSN Code of Connection, Practice and/or Interconnection from the technical, physical and administrative perspectives
- Political constraints (at a regional level)
- The transfer of some responsibilities to Central Government and /or PSN service provider
- Commercial considerations
- Loss of in-house skills and expertise

Contact us:

Further details, including case studies, presentations and references are available from Nigel Strutt. Please call 07780 526195. Head office; 41, Barry Avenue, Bicester, Oxfordshire. OX26 2DZ.

Email: nigel.strutt@advisec.co.uk