

Report Reference Officer Decision – IT Network Renewal

Date: 08/01/25

Author: Dan Pobjoy

Executive Summary:

This report details the decision for the procurement of new network infrastructure, replacing equipment that is now either end of life or close to end of life, thus not receiving the necessary security patches and updates, and for the design, configuration and implementation works to be carried out by Intergence Systems Limited.

The reader should be aware that the re-design and installation and support of our corporate ICT network is effectively giving the chosen contractor “the keys to the kingdom” in respect to unfettered access to our cyber-security and council-wide data storage/ data flows. Consequently, the importance of proven cyber-security and information governance and assurance expertise and a trust-based contractor relationship cannot be over-stated.

Tendring District Council has been working with Cambridgeshire-based Intergence Systems Limited for the past 8 years. Their knowledge and expertise in supporting the Council’s complex blend of critical systems and supporting infrastructure has been repeatedly proven. This, in turn, provides the high levels of business continuity and resilience that the Council relies upon to deliver services to residents.

The due diligence process and procurement decision to undertake a direct award to Intergence included key considerations around: proven cyber-security capabilities, information governance and data security, level of access, proven technical expertise, local knowledge ensuring network integrity, value for money, social value, trust, skill-sharing and partnership engagement.

Government level Security Clearance (SC) at Project, Design and Support Levels - (Security Clearance conforms to BS7858). The company also has the following Security Governance and Risk Certifications: ISO:27001, ISO:9001, Cyber Essentials Plus are also key assurance considerations.

A key qualitative consideration has been the very significant and real strategic cyber security risks surrounding the design and implementation of the new network infrastructure and configuration, together with the potential for catastrophic Council reputational loss should we suffer a large loss of data or cybersecurity breach.

The total costing of the solution including new infrastructure for the estate and installation, setup, configuration, testing, High-Level and Low-Level Designs, test plans and results are £234,000. In this regard the reader should note that the £233,337 replacement costs comprises;

- 1) £182,000, replacement hardware costs (*)
- 2) £52,000 Intergence Systems Ltd network re-design and implementation/ installation costs

* For reasons of cyber-security this report does not name the 3rd party hardware suppliers chosen to replace our aging network hardware.

In accordance with Council’s Budget and Policy framework this procurement will be a direct award via the G-Cloud 14 framework LOT 3. Cabinet previously approved the budget for IT network renewal costs report A.2 FINANCIAL PERFORMANCE REPORT 2024/25 – GENERAL UPDATE at the end of July 2024 refers.

Background:

The Council has had a Cyber Security and Managed Network Service contract with Intergence Services Limited for the past 8 years, during which time, additional services have been added, including:

- Wireless Managed Service Support
- End-Point Asset Management Software
- Server Monitoring Licenses

During the lifecycle of the contract, the council has benefited from Intergence' support and specialist resources to radically evolve the council's digital estate to the flexible, resilient and remote working infrastructure that we utilise today. Transformational works include: migrating 90% of our estate to the Microsoft Azure platform, implementing a new and resilient Wi-Fi, continued rollout of replacement updated network hardware and data transport mechanisms, migrating our telephony estate from Microsoft (MS) Skype for Business to MS Teams and delivery of resilient and secure remote working capabilities.

In addition to providing specialist expert resourcing and support, from a perspective of the 'official' and 'official sensitive' data that we hold in guardianship on behalf of our residents and customers to deliver the range of local authority duties and services the council must engage with a partner whom they can trust implicitly.

Giving a partner the levels of security access necessary to support our infrastructure is effectively giving them "the keys to the kingdom" - albeit with the appropriate levels of monitoring and reporting.

Due to the size, complexity, value and security concerns around the works need to design and implement the upgrade of our network infrastructure, we need to ensure the correct company is contracted to complete the work with the correct knowledge, skillset, certifications and expertise. To ensure this, we have carried out some due diligence using filters for needs on the G-Cloud 14 framework.

The checks and filters we used were:

- Searching under Lot 3 (Cloud Support) of the G-Cloud 14 Framework for "Digital cloud transformation and network specialists" – Producing a result of 48 including 31 suppliers)
(<https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/search?q=Digital%20cloud%20transformation%20and%20network%20specialists&lot=cloud-support>)
- Created a spreadsheet of these 31 suppliers showing their minimum, maximum and mean day rate.
- Filtered out suppliers from this list that does not state they carry out the works we need (ie they cover only Citrix, they work in healthcare only etc) – 31 suppliers down to 17.

After these first initial checks, Intergence Systems Limited were the only company of the 17 remaining that we had previously worked for and placed midway for the mean day rate.

To further filter down we carried out further checks on G-loud 14:

- We wanted to ensure the company wasn't a reseller, where they had user support through email, online and phone, the certifications they held were ISO/IEC 27001 (Service security) and Cyber Essentials Plus and Staff Security Conforms to

BS7858:2019 – This reduced the Suppliers to 3 of which Intergence were the only ones left from our previous filter from the spreadsheet. (Search String - [Search - Digital Marketplace](#))

- To further reduce we also filtered on the search term “MDR” (Manage, Detect and Response) a search term used for cyber security support and mitigations. This left just 1 supplier – Intergence Systems Limited ([Search - Digital Marketplace](#))

During our contractual relationship over the past 8 years and to date, Intergence have proven repeatedly: their professional competence and capabilities, depth of knowledge/ expertise, independent ‘agnostic’ IT system appraisal/ advice.

Key to the strength and value of these contract has been Intergence’ agility and willingness to respond quickly in support of our changing requirements, the ‘added value’ that they provide in terms of pre-agreed and ‘ad hoc’ and free staff support and transfer of skills. In this regard, the knowledge and expertise that Intergence has shared with the Council’s internal IT Team including:

- Development – working with the council’s IT Development Team to create, design and build new IT systems which in turn generate real financial savings through; not procuring external systems, generating staff efficiencies, further evolving the council’s services to meet ever-increasing resident/ customer expectations. This was prominent throughout the pandemic when new Covid-related systems needed to be created in a short time span to meet central government deadlines
- Cloud Computing – working with the Technical IT team to manage and maintain the move from in-house hosted infrastructure to our new Microsoft Azure Cloud Infrastructure (covering the adopted ‘Cloud First Strategy’)
- Cyber Security and Resilience – working with the Technical and Cyber IT team to strengthen our cyber security, offering new tools and techniques available to us and providing a Security Operations Centre (SOC) to mitigate against the very increasing threats of a cyber-attack/incident.

The chosen brand of the hardware that Intergence will provide within the implementation of the new network is a Leader in Gartner Magic Quadrant for the fifth year in a row. The hardware chosen to install will align with the software we have and grant us the ability to evolve our cyber estate further, utilising additional cyber threat intelligence software and visibility.

The fees and charges are comparable with IT industry market rates. Additionally, and as expanded upon within this report, these charges are supplemented by the range of ‘value-add’ and free training/ development and knowledge-exchange resource services provided where other more commercially aggressive companies demanded payment.

As part of the works, Intergence will also be upgrading some of the older infrastructure at both the Sheltered Housing Schemes and the Leisure Centres Free of Charge.

In summary, as a trusted technology support partner, Intergence have proven and continue to prove: their technical specialist expertise and capabilities, their business agility and support capabilities (during very demanding times), their willingness to work alongside council IT resources sharing knowledge/ information and assisting the development of new skill-sets. In addition, their fees and charges are comparable with IT industry market rates arguably supplemented by the range of ‘value-add’ and free services they provide where other more commercially aggressive companies would have demanded payment.

This short report and officer decision proposes that the Council, procures all the required network infrastructure, and for the design, configuration and implementation works to be carried out by Intergence Systems Limited.

Reasons for the decision:

Awarding Intergence Systems Limited the works to design, configure and install the updated network infrastructure will offer many benefits, including:

1. **Minimal service disruption and business risk** – awarding the works to Intergence systems Limited, a company we have been working with for several years, have a knowledge and experience of our network and configuration and who we have a highly trusted relationship with, will enable the service and support of all our critical systems to be fully functional during the works. Moving to a new supplier will be a prolonged process and may risk a period of unsupported systems or exposure to poor technical support knowledge/ capabilities.
2. **Value for Money And Business Continuity** – Intergence carrying out the work ensures all the extra services and monitoring is kept with one supplier thus ensuring value for money, continuity of service plus a range of ‘value-add’ free services.
3. **Resilience enhancements** – The services and the knowledge and expertise provided by Intergence ensure the Council has a highly resilient, modern and enabling infrastructure.
4. **Cyber Protection and Support** – Alongside the council’s IT and cyber team, Intergence provide resources, processes and technology to continuously monitor/ improve our cybersecurity and response to cybersecurity incidents.
5. **Single Point of Support** – The managed service contract and cyber security contract we currently have with Intergence covers a complex mix of technologies and systems all supported by one provider. These include: Wide Area Network (WAN), Local Area Network (LAN), Wi-Fi
6. **Proven Knowledge and Expertise** – working with the said company for several years and on a number of high-level projects (as previously outlined) has proven Intergence knowledge and expertise in the field.
7. **Security, Governance and Risk** – Intergence have Government level Security clearance (SC) staff at Project, Design and Support Levels (Security Clearance conforms to BS7858). The company also has the following Security Governance and Risk Certifications: ISO:27001, ISO:9001, Cyber Essentials Plus.
8. **Social Value** – Intergence have previously and continue to provide Cyber Security support and guidance to local businesses through the Tendring for Growth Platform. They have also provided network coverage for the Clacton Airshow at previous events.

All the above factors sign-posted officer thinking that awarding the works to Intergence Systems Limited is the correct decision. This in turn gives confidence and trust in professional competence and confidence in delivering the required technical reliability and resilience this key service requires.

A key qualitative consideration has been given to the very significant and real strategic cyber security risks surrounding the upgrading of the network, together with the potential for catastrophic Council reputational loss should we suffer a large loss of data or cybersecurity breach.

The Council’s IT Technical Operations Manager independently recommended to the Head of IT and Resilience Service that the new contract be awarded based upon the above rationale.

Financial Summary:

The total costing of the solution including new infrastructure for the estate and installation, setup, configuration, testing, High-Level and Low-Level Designs, test plans and results are £234,000. In this regard the reader should note that the £233,337 replacement costs comprises;

- 1) £182,000, replacement hardware costs (*)
- 2) £52,000 Intergence Systems Ltd network re-design and implementation/ installation costs

In accordance with Council's Budget and Policy framework this procurement will be a direct award via the G-Cloud 14 framework LOT 3. Cabinet previously approved the budget for IT network renewal costs report A.2 FINANCIAL PERFORMANCE REPORT 2024/25 – GENERAL UPDATE at the end of July 2024 refers.

Legal:

This proposed investment is in accordance with the Council's Budget and Policy framework. The procurement route will be through the UK government G-Cloud framework (Lot 3) which is fully compliant with the Council's Procurement Procedure Rules.

End