

## Scrutiny questions for ICT and responses

### 1. How has performance been compared to the Business Plan?

The KPI's being reported against show that throughout the last 3 quarters 3C ICT are exceeding or within tolerance (10%) of the agreed targets.

### 2. What are the biggest disappointments and successes in your time in role, so far?

Since Sept 2019 – Improved Infrastructure and risk mitigation, including the roll out of Council Anywhere technology across the 3 councils. SCDC in particular was a success as they were the first to complete the roll out of new devices and set the standard for the 'Champions' within the business areas. The EastNet project (migration of network links and services) has taken longer than we'd like and due to late agreements. Therefore an accelerated schedule of work was developed to try and catch up before the expiry of the legacy contract. The MLL firewall migration work in Dec also caused unexpected and significant disruption.

Meeting the PSN accreditation requirements following extensive infrastructure improvement and consolidation projects.

### 3. Where are our biggest vulnerabilities?

There is still a lot of technical debt from legacy systems and services that weren't known or declared when 3C ICT was formed. Cyber security is an ever-present risk, even though good technical controls are in place and we continue to meet with accreditation requirements.

Resource pressures including problems with recruitment for technical roles.

Short term risks and vulnerabilities – supporting Covid-19 planning is taking a lot of resources and supply chain issues are hitting us now with hardware (laptops and monitors in particular) lead times.

### 4. Where are we in considering RPA (Robotic Process Automation)?

Each council are at different stages. SCDC have not got any specific plans or developments at the moment or in the pipeline for the next 6 to 12 months.

The SCDC Transformation team will be able to advise on longer term plans.

**5. Where are the biggest benefits from new ICT projects going to arise in the next two years?**

Biggest benefits will come from properly and fully exploiting the technology and platforms that have just been deployed. E.g. Council Anywhere and wider use of integrated suites of tools such as Microsoft O365, Teams, Power BI, office suite, Unified Communications. Whilst 3C ICT can implement the solutions, it's the transformation teams and service areas who will be key in ensuring that benefits are realised.

**6. Have we now got:**

- **an IT Security Policy?** – Yes – was published by information governance team last year. The document will go through regular reviews to keep in line with changes in legislation, new and emerging threats and as tools, equipment and behaviour changes.
- **a Business Continuity Plan?** – There's a plan covering 3C ICT and our services (IT Service desk, desk top support, applications support, Network and infrastructure service operations, IT Purchasing, but BC plans sit with service areas to create and maintain. Where necessary, underpinned by ICT services. However, some plans should be built around the scenario where ICT services are not immediately available.
- **a Risk Assessment Plan?** – Risk assessment plan for Infrastructure has been completed for (each council). Separate Application risk and Cyber security risk assessments also completed.
- **a Disaster Recovery Plan?** – DR plan is in place and built around the 2 site architecture for the data centres.

**7. What is our backup process? Is any of it cloud based, are there plans to for it to be so?**

We use an Enterprise grade solution for backup with integrated with other tools for monitoring and management. For services and systems hosted on site, the backup technology and processes are built around replication, snapshots and Virtual Server technology.

External cloud-based backups may apply to some externally hosted systems where we have Software as a Service (SaaS) agreements in place where their services are cloud based. These will vary from supplier to supplier. We

also have email messages journaled via a 3<sup>rd</sup> party tool, primarily for archive purposes, but also provides security and backup benefits. As more services are provided as hosted or cloud based, backups will inevitably move in line with those service offerings.

**8. What are the SLA's to be backup to BAU for each business area?**

SLA's are not specific to individual business areas. Backups are kept at each main Data Centre site and are immediately available for use. Application aware backups are also available for some systems enabling shorter recovery times in some cases. Restore times for individual servers are in the order of a hours, but fast recovery is available using the backup technology we've deployed depending on the nature of the failure or incident.

**9. When was the last full DR test performed and what were the results?**

If there has not been a DR test in the last year, what are the plans for one. Would you be able to provide an overview of the tests? Last DR use was Nov 2018. Backups are used on a regular basis (weekly) for file and data recovery purposes. Plans are being developed to carry out a DR test for the new network infrastructure now that we've moved from VMB CPSN to MLL East Net. This is planned to take place within the next 3 to 4 months.

**10. Do we have a full system map with single points of failure identified?**

Various documentation exists covering different areas of technology – Network topology, Server config and management tools and logical diagrams, physical asset management records for servers/hosts.

**11. Do we have a list of assets held?**

A Hardware asset register is in place. In Nov 2019 associated tools, processes and procedures were audited as part of the 3C Shared services audit programme – This concluded that there was a good level of assurance with only a few low and medium actions to complete.