Report author: Bev Fisher
Tel: 07891 275318

Report of the Head of Service Delivery ICT

Report to Scrutiny Board (Strategy & Resources)

Date: 9 March 2016

Subject: Scrutiny Inquiry into ICT Capacity – Session 3

Are specific electoral Wards affected? If relevant, name(s) of Ward(s):	☐ Yes	☒ No
Are there implications for equality and diversity and cohesion and integration?	☐ Yes	☒ No
Is the decision eligible for Call-In?	☐ Yes	☒ No
Does the report contain confidential or exempt information? If relevant, Access to Information Procedure Rule number: Appendix number:	☐ Yes	☒ No

Summary of main issues

To provide Scrutiny Board (Strategy & Resources) with the information required to undertake the third session of the inquiry into ICT capacity.

This report explores the expectation in Council of hours of service, reliability and availability.

Recommendations

Scrutiny Board is requested to:

a) Note the contents of this report

b) Make recommendations as deemed appropriate

1 Purpose of this report

1.1 To provide Scrutiny Board (Strategy & Resources) with the information required to undertake the third session of the inquiry into ICT capacity

1.2 The report explores the expectation in Council of hours of service, reliability and availability.

2 Background information

2.1 The Scrutiny Board agreed the terms of reference in October 2015, three enquiry sessions were planned, this being the third.

2.2 The third scrutiny session covers the expectation in Council of hours of service, reliability and availability including:

- Review of current ICT service level agreement (hours of cover, availability) and whether this is appropriate given an increasing demand and expectation from services for extended or even 24 hrs x 7 days x 365 days a year services.
- Review previous investment decisions in relation to system resilience/support and whether further investment may be required to support increased demand for extended or even 24x7x365 services.
- Review of systems that have to be shut down for overnight processing (or other reasons) and the impact this causes.
- Review whether business continuity arrangements in service areas (to deal with unexpected or planned system downtime) are sufficient and effective.

3 Main issues

3.1 The current ICT Service Level Agreement is measured 24x7x365 but excludes agreed planned downtime/batch processing windows). Details of service level availability are contained in Appendix A.

3.2 There are pre-agreed planned maintenance windows during which updates such as patches are applied or servers are rebooted..

3.3 ICT standard support hours are Mon - Fri 08:00 – 17:30.

3.4 There is a small team who work shift hours (24x7 except for overnight Sat 19:15 to Sun 08:30 and Christmas day) to manage batch processing and to provide a level of monitoring of systems.

3.5 There is a limited out of hours support service provided via an ‘on-call’ arrangement with a number of teams providing cover on a voluntary paid basis to deal with major issues. Since its introduction this has enabled a number of issues to be fixed overnight thereby avoiding significant business impact at the start of the next working day.

3.6 There are a number of systems which have to be taken down to perform batch processing or for a backup. Details of these are in Appendix B.

3.7 When systems fail, we need to be notified of the failure in order to mobilise teams to resolve the issue. This can be via automated alerts, manual monitoring or through a call to the ICT Service Desk.

3.8 Deploying software updates to some systems involves taking the application offline. For systems such as our website (leeds.gov.uk) this means an interruption to service.

3.9 For Council services who operate outside of the 'normal' business day (Sports Centres, Libraries, Theatre's) planned downtime in evenings or on weekends will affect them at what can be a busy period.

3.10 There has been investment through the ICT Essential Services Capital scheme to improve resilience and this has been built in at a number of levels including the network links, data centre facilities (power/cooling) and server components. Appendix C shows Resilience techniques used at a system level.

3.11 Automatic failover of applications between data centres is not currently provisioned.

3.12 The Council has previously been presented with options and outline costs to enable automatic failover of applications. This has been done in 2010, 2012 and 2014 and the decision has been that availability and hours of service are 'good enough' when considering cost versus benefits.

3.13 A paper was taken to CLT in Sep 2015 to describe the levels of resilience in place, to advise on work underway to identify critical ICT systems and to discuss the need for further investment to enable automatic failover of applications between data centres. Appendix D contains this paper and the agreed outcomes.

3.14 A separate review has been undertaken of how the Council could improve availability of our website (Leeds.gov.uk) through reducing or removing the need to close the site whilst software updates are applied and through enhancing out of hours support. A project is underway to progress this.

3.15 Work has been undertaken to create Business Continuity Plans for critical services and to ensure these are regularly reviewed by the service areas. Specific guidance is given for service areas to consider how they would continue operating in the event of the loss of technology (phones, applications, PCs). The robustness of those BC plans (as it relates to loss of technology) should be regularly reviewed and tested by service areas.

3.16 For critical applications, regular Disaster Recovery Tests are undertaken to test that, in the event of a loss of a data centre or servers, the application and data can be successfully recovered to an alternate site or server.

4 Equality and Diversity / Cohesion and Integration

4.1 An equality and impact assessment has not been completed at this stage of the enquiry.

4.2 Equality and diversity will be a consideration throughout the Scrutiny Inquiry. Due regard will be given to equality through the use of evidence, written and verbal, outcomes from consultation and engagement activities.

4.3 Where an impact has been identified this will be reflected in the final inquiry report, post inquiry. Where a Scrutiny Board recommendation is agreed the individual, organisation or group responsible for implementation or delivery should give due regard to equality and diversity, conducting impact assessments where it is deemed appropriate.

5 Recommendations

5.1 .Scrutiny Board are asked to note the ICT service levels, hours of cover and on-call arrangements and provide a view on their adequacy to meet Council needs.

5.2 Scrutiny Board are asked to note the limitations of some systems to be able to operate 24x7 and to note the need for ICT to have planned downtime in order to adequately maintain services.

6 Background documents[1]

Appendices

A Service Level Achievement

B System downtime for batch and backups

C System Level Resilience techniques

D Data Centre & ICT Services Resilience paper

Appendix A – Service Level Achievement

Service desk	Target	October	November	December	January	February
SLA 01 - % of incoming calls answered within 30 seconds	>= 70%	43.75	53.25	59.64	62.87	58.49
SLA 02 - % of calls queued to an operator but abandoned prior to pickup	<= 7%	10.08	5.50	2.83	3.08	1.62
SLA 03 - % incidents resolved at first point of contact	> = 70%	78.43	76.25	78.66	81.52	77.37

Incident management	Target	October	November	December	January	February
SLA 04 - % of CRITICAL priority incidents met with target time to resolve	>= 80%	No incidents	100.00	No incidents	100.00	No incidents
SLA 05 - % of HIGH priority incidents met with target time to resolve	>= 80%	60.00	0.00	66.67	75.00	100.00
SLA 06 - % of MEDIUM priority incidents met with target time to resolve	>= 80%	87.30	92.11	94.12	98.10	94.06
SLA 07 - % of LOW priority incidents met with target time to resolve	=> 80%	93.07	91.52	93.23	94.34	92.98
Total number of Incidents reported in reporting month		4106	4548	3853	4488	4421

Corporate ICT offering	Target	October	November	December	January	February
SLA 08 - Network login password reset	>= 96%	97.28	94.12	93.55	97.24	95.10
SLA 09 - Percentage of all incidents categorised as Desktop PC.	<= 5%	2.97	2.66	2.47	2.97	2.48
SLA 10 - Percentage of all incidents that are categorised as Laptop PC	<= 5%	3.91	3.58	3.76	3.74	3.02
SLA 11 - Percentage of all incidents that are categorised as Tablet PC	<= 2%	0.12	0.11	0.05	0.00	0.04
SLA 12 - Antivirus protection. % of virus attacks repelled.	100%	100	100	100	100	100

Customer satisfaction	Target	October	November	December	January	February
SLA 31 - How satisfied were you with the level of customer service received in relation to this incident?	>=5 out of 7	6.56	6.59	6.56	6.72	6.60
SLA 32 - How satisfied were you with the time taken to resolve this incident?	>=5 out of 7	6.55	6.55	6.52	6.65	6.52
SLA 33 - How satisfied were you with the overall service received specifically for this incident?	>=5 out of 7	6.53	6.59	6.56	6.71	6.51
SLA 34 - Outside of this incident, how satisfied are you with the services provided by ICT overall?	>=5 out of 7	6.08	6.25	6.13	6.32	6.16
Total number of surveys completed in reporting month	n/a	244	214	193	233	267

Availability of key services	Target	October	November	December	January	February
Network Data - Communications	99%	100.00	99.00	100.00	99.99	99.99
SLA 13 - Contact Leeds	99%	100.00	100.00	100.00	100.00	100.00
SLA 15 - Iclipse	99%	100.00	100.00	100.00	100.00	100.00
SLA 16 - e-Mail Service	99%	99.76	100.00	100.00	100.00	100.00
SLA 17 - ESCR	99%	100.00	100.00	100.00	99.27	100.00
SLA 18 - FMS	99%	100.00	100.00	100.00	99.27	99.42
SLA 19 - Internet Access	99%	100.00	100.00	100.00	99.27	100.00
SLA 20 - Academy CT & Benefits	99%	100.00	100.00	86.70	84.03	99.80
SLA 21 - Leeds City Council Website	99%	100.00	100.00	100.00	99.27	100.00
SLA 22 - Network Security PDMZ (Partial de-militarised zone)	99%	100.00	100.00	100.00	99.27	100.00
SLA 23 - NetApp File and Data Access	99%	100.00	100.00	100.00	100.00	100.00
SLA 24 - Orchard Housing Services	99%	95.68	100.00	99.15	99.27	100.00
SLA 25 - Insite	99%	99.03	100.00	100.00	100.00	99.47
SLA 26 - SAP/HR Payroll	99%	100.00	99.71	100.00	99.27	100.00
SLA 27 - Landline Phone Network (Voice)	99%	99.95	99.57	100.00	98.87	100.00
SLA 28 - Mobile Phone Network	99%	100.00	100.00	100.00	100.00	99.68
SLA 29 - User's Desktop Environment	99%	100.00	100.00	100.00	100.00	100.00
SLA 30 - ASC Client Information System (CIS)	99%	100.00	100.00	100.00	100.00	100.00
SLA 31 - Children's Framework-i	99%	96.18	100.00	100.00	100.00	100.00
SLA 32 - ICT4Leeds	99%	100.00	100.00	96.25	99.27	99.76
SLA 33 - Income Management	99%	100.00	100.00	100.00	99.27	100.00

Mobile working services availability	Target	October	November	December	January	February
SLA 34 - Smart Phones & Tablets	99%	100.00	100.00	100.00	100.00	100.00
SLA 35 - Virtual Private Network (VPN)	99%	100.00	100.00	100.00	99.27	100.00
SLA 36 - Skype For Business	99%	100.00	100.00	100.00	99.27	100.00

Appendix B – System downtime for batch and backups

Applications taken down to do batch processing:

System	Batch / backup window
Academy (Council Tax, Debt Management, NNDR)	19:00-07:00 weeknights, 14:00 Sat-07:00 Mon
Orchard Housing	00:00-07:00 weeknights (but to 08:00 Sat morning) and 08:30-11:00 Sun

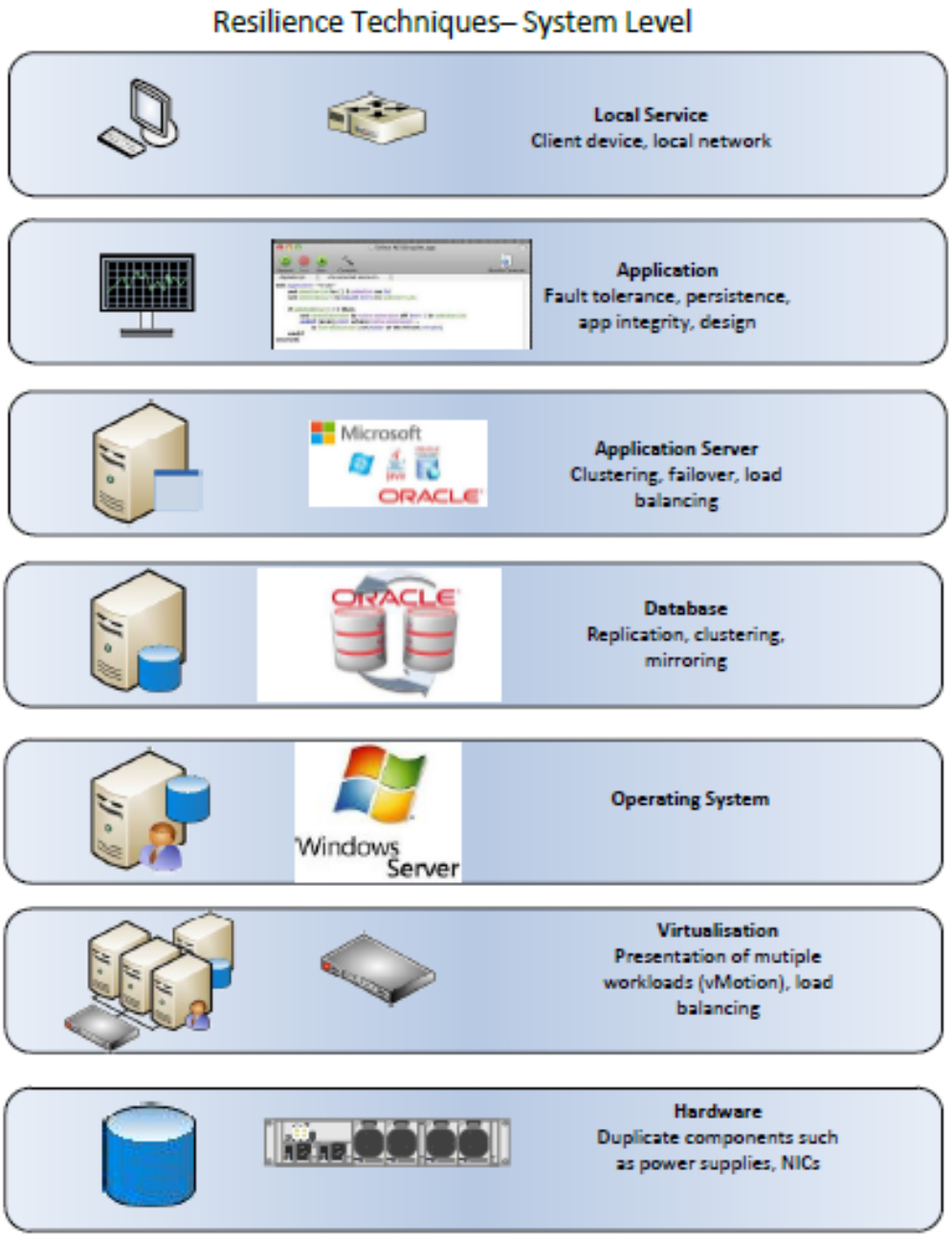
Full backups performed for which application has to be taken offline:

Db	Application	Cold backup window (from)	Days
PIL	SAP(connection to HMRC)	05:00	Sat
SSL	Translations	20:35	Mon-Fri
ESCRDWL	Data warehouse	19:50	Fri
HSL	Housing Stock	19:15	Mon-Fri
HSL	Housing Stock	Sunday evening after batch	Sun
CRMDWL	Data warehouse	19:50	Mon-Fri
IFAL	Integrated Financial Application	18:55	All bar Fri
IFAL	Integrated Financial Application	21:00	Fri
FML	Financial Management System	19:00	Mon-Fri
FML	Financial Management System	14:00	Sat

We also reboot ALL the Unix servers in the M5000 hosted estate every 9 weeks – some of these reboots can take the application down for up to 4 hours.

We also reboot the Unix servers not hosted in the M5000 estate every month – these reboots are typically up to 20 minutes in duration

Appendix C – Resilience Techniques



Appendix D – Data Centre & ICT Services Resilience

Date of meeting:

CLT lead: Alan Gay

Paper author: Dylan Roberts

Paper title: Data Centre and ICT Services Resilience
Category of paper (please mark A or B): B

Corporate Leadership Team (CLT)

Purpose:

To advise CLT of the level of resilience that will be in place for key systems and services following the work planned in this year's ICT Essential Services Programme.

To provide an explanation of the current business continuity arrangements in place within services to ensure continuity of operation in the event of failure or planned closure of ICT systems.

To appraise CLT of the work underway to review critical services and the desired availability of the ICT systems underpinning them.

To seek CLT approval for development of options and outline costs to meet identified ICT system availability requirements.

Key issues or outcomes:

Some services have a critical reliance on the Councils ICT systems and the expectation from some is for ICT systems (the applications and underpinning technology) to be available 24 x 7 with the impact of any technology failure eradicated and no need to shut systems to apply upgrades.

Necessary upgrades are undertaken during 'planned downtime' over weekends and overnight to minimise disruption during the working week. However, some services e.g. Sport Centres, are busiest at these periods and are impacted by this.

The current funding and associated staffing resource within ICT covers the service hours of 0800 to 1730. Budgets and staff numbers have decreased over a number of years and any requirement for increased levels of cover will require further investment.

ICT have an on call service from some key teams enabling issues that occur out of service hours to be fixed before the start of the next business day. This out of hours cover is

provided on a voluntary basis and it is not mandated.

There are some areas of expertise where there are single people (points of failure) with specialisms and it is not possible to extend the hours of cover without significant increases in the teams.

The two main data centres that service council systems are located at Civic Hall and Apex Centre and services and systems are spread across both sites.

There is a high capacity network link between the two data centres and a level of resilience built into shared infrastructure components such as server devices, server clusters and network components e.g. redundant power supplies. Failures of individual components do occur however the resilience ensures no disruption is caused.

ICT infrastructure is being implemented which provides the building block upon which increased resilience could then be built for individual ICT applications where this is deemed an absolute requirement. To make the Councils business applications resilient will require further investment to 'mirror' the application components across both data centres.

When complete, by the end of the financial year, this will deliver the following:

- Network resilience across data centres. This means if a network component is affected services would continue to operate.
- Server and storage infrastructure will be the same in both Civic and Apex but with differing workloads and applications running at each site
- If there was a significant failure at its host datacentre, a service can be recovered in the other datacentre through rebuilding services and restoring data. For an individual system this would typically be within a day however in the event of recovering multiple systems then priority would be given to critical systems.

Things that are **not** covered by the current Data Centre Resilience work

- Provision of instant failover on individual applications/services with no downtime for users
- Many of our network lines to end sites are single lines with limited resilience.

This work in itself involves some level of disruption which is being undertaken over weekends at present.

The cost of improving resilience, above that above, **for all systems** is significant and would involve capital and revenue investment in the millions in terms of equipment and people. Whether a 24 x 7 service from ICT is something that all services actually **need** must be considered. Costs have previously been provided to give a level of additional support to some services and never taken forward.

There are also a number of challenges relating to the ongoing recruitment and retention of suitably skilled resources into ICT Services to support 'Lights On' services which will need to be addressed if extended support hours are required.

Some of the ICT systems and services in the Council are not architected in a way which enables them to be available 24 x 7. In many cases they are reliant on batch processing overnight to clean up databases and so forth which requires the system to be down. These

restrictions will need to be factored into any requirements for 24x7 services.

Whilst a level of resilience can be built, no ICT service provider provides a 100% guarantee of service availability and it is inevitable that there will be some downtime for services in future. Existing levels of service availability regularly exceed 99.1%.

There are business continuity plans (BCP) in place for 86 services across the Council who are deemed critical or key. The BCP plans contain specific sections around the arrangements a service will adopt in the event of the loss of ICT systems and services including :

- Loss of the data or voice connection to their building
- Loss or theft of equipment such as PCs, printers, screens from the services building
- Loss of a core critical business application (i.e. the application is not working irrespective of which site the service is based at)
- Loss of ability to log on to PCs
- Loss of access to data (L drives/SharePoint)

The risk of major ICT failure is identified and regularly reported in the Corporate risk register LCC15.

Identified risks or opportunities:

Work underway as part of this year's ICT Essential Service Programme will provide the base infrastructure upon which individual system resilience can be developed as detailed above.

Investing more in ICT services from an infrastructure and staffing point of view provides the opportunity of increased availability and less service downtime. This will cost a significant amount of money.

Therefore, Heads of IM&T are undertaking a detailed service criticality exercise with all areas across the Council to ascertain with each the must have requirements and the business case for the provision of additional system resilience for their systems. (e.g. Frameworki, FMS, SAP, Website etc.) This will inform a more detailed Council business case that may provide variable levels of resilience and support for different services as required.

Actions or recommendations:

CLT are asked to :

- Endorse the Service Criticality Assessment work and commit to provide resource from services to work with the Directorate IM&T teams in assessing requirements for 24x7 services and support and improved resilience.

- CLT to consider and agree one of the following options :

Option 1
An infrastructure set up with full fail over capability for **all services** which means that when service is interrupted at one Data Centre, it will automatically flip over to a service running in parallel at the other data centre with limited user impact. This is likely to require a multi-million pound investment.

Option 2
An infrastructure set up to provide the "best possible" for those services identified as absolutely critical (as identified in the Service Criticality Assessment). This may be a mixed economy of those which may be able to "flip over" and those that will be recovered by the soon to be delivered set up. This is likely to require a significant investment to be determined.

Option 3
Accept the resilience that will be delivered by the current work. This is where individual systems would typically be recovered within a day however in the event of recovering multiple systems then priority would be given to critical systems. Investment for this is already built into the Essential Services Programme.

- If Option 1 or 2 are taken agree that further work be undertaken to develop outline proposals and costs in support of either Option 1 or Option 2.

Outcomes agreed at CLT meeting
An acceptance that, due to the way the majority of our systems are architected, the resilience provided by the current work programme, which will be completed by the end of Feb 2016, is as good as we are going to get. **This is where individual systems would typically be recovered <u>within a day</u> however in the event of recovering multiple systems then priority would be given to critical systems.** Investment for this is already built into the Essential Services Programme.

However, Heads of IM&T working with Nigel Street (Resilience & Emergencies Team), will be engaging with Directorate Management Teams ASAP using a Service Criticality template in order to do determine which are the **most critical systems.** The criteria and information required to consider in making these decisions are those that relate to the cost of downtime, the risk to people and what continuity arrangements can be put in place should there be a failure.

ICT Services will then determine what additional infrastructure is required "just in case" for the recovery of the most critical systems to one data centre.
NB. This is likely to be to the level (as noted above) **where individual systems would typically be recovered <u>within a day</u> however in the event of recovering multiple systems then priority would be given to critical systems**

However, if for some individual systems there is the opportunity to improve this, perhaps through upgrades of the application, re-architecting or other then it will be determined and the costs for that reported back.

The conclusion of this work will result in a "cost/benefit" paper to CLT by February time ready to feed into the Capital Programme for 2016/17.

NB. It is important that all DMTs assess their Business Continuity Plans on a regular basis which must also include contingencies and mitigations against ICT failures which will, although not often, happen.