Manchester City Council
Report for Information

Report to: Audit Committee - 3 September 2018

Subject: ICT Assurance Update: Disaster Recovery Planning and Public Service Network

Report of: The Chief Information Officer

Summary

In October 2017 Audit Committee were provided with an update on plans to achieve ICT Disaster Recovery (DR) capability for the Council. Members requested that a further update be provided to Committee as this work progressed. Work is underway to establish the DR capability by the end of September 2019 and this report sets out the associated approach and timescales.

This approach means that three Internal Audit recommendations relating to DR are no longer deemed relevant; as they will be superseded by the new solution. This report sets out the context for this proposal.

Audit Committee on 31 July confirmed that the DR report should also include an update on actions being taken in respect of access to the Public Service Network (PSN). This update is set out in the report.

Recommendations

Audit Committee are asked to consider the assurance provided by the update report.

Wards Affected: All

Contact Officers:

Name: Bob Brown - Chief Information Officer
Email: bob.brown@manchester.gov.uk
Telephone: 0161 234 5998

Background documents (available for public inspection):

The following documents disclose important facts on which the report is based and have been relied upon in preparing the report. Copies of the background documents are available up to 4 years after the date of the meeting. If you would like a copy please contact one of the contact officers above.

- DR Report to Audit Committee October 2017
- Outstanding Audit Recommendations report to Audit Committee July 2018

- ICT Update Report to Scrutiny Committee July 2018

1. Introduction and Background

1.1. Disaster recovery (DR) and business continuity planning are integral parts of the overall approach to risk management. Since all of risks cannot be eliminated, organisations implement disaster recovery and business continuity plans to prepare for potentially disruptive events.

1.2. Both processes are equally important for the Council because they provide detailed strategies on how services will continue to operate during severe interruptions and in the aftermath of major incidents and disasters. At present the Council has no formal disaster recovery capability and a programme of work is underway to address this issue to ensure systems and services are available.

1.3. A report to Audit Committee in October 2017 set out the approved strategy to develop a disaster recovery capability; and at the same time to improve the underlying resilience of the Council's ICT infrastructure to help minimise the risks of interruptions and incidents.

1.4. Along with resilience and disaster recovery, ICT security is also a key risk to any large organisation. One of the ways in which the Council's ICT security arrangements are reviewed and assured is through a programme of ongoing Public Services Network (PSN) compliance that is led by the Cabinet Office. This enables the Council to access the PSN which helps public sector organisations work together, reduce duplication and share resources.

1.5. This report update Audit Committee on progress to date in respect of DR and PSN.

2. Data Centre Programme Update

2.1. The overall objective of the Data Centre (DC) Programme is to ensure high availability of critical business applications, services and ICT infrastructure. The programme will remove single points of failure within ICT infrastructure through the delivery of a resilient and robust data centre solution for the Council. The programme is based on the operation of services from two active data centres rather than a 'traditional' model of a primary and back-up data centre. This model means that each data centre will always be active and in the event of interruption or disaster at one, the other centre will act as an almost immediate failover solution.

2.2. The programme is made up of three projects:

- Core Infrastructure Refresh (delivery phase)
- Network Design and Implementation (procurement phase)
- Data Centre Facilities and migration (build phase).

2.3. The DC programme also includes the removal of the current manual telephony failover to Salford City Council's Data Centre; and will 'lift and shift' the current telephony solution from Salford and Sharp in to the new data centres whilst the procurement of a new unified telephony solution is underway. The DC

programme is now in the delivery phase and services are expected to be operating from the two new data centres by September 2019.

2.4. The contract with the new data centre facility provider, UKFast was signed on 2 July 2018. Council ICT services will transition from the Sharp data centre into two separate disaster recovery (DR) equipped data centres within Manchester that the Council will rent as a managed service facility. Council services will be delivered from the two 'active:active' data centres with DR capability for critical services and applications. In the new design if a single data centre becomes unavailable, critical systems will be restored in the second data centre (if not already running from there).

2.5. The Core Infrastructure Refresh Project is in the delivery phase and progressing well. All virtual servers will be running on new technology by October 2018 in the Sharp Data Centre, providing greater resilience prior to the move to the new data centres. The new infrastructure will replace existing old technology, including storage and backup solutions and will be split across the two new data centres delivering high availability and DR capability for critical applications and services. The migration of live environments are well underway and on track to migrate by October 2018.

2.6. This approach will result in two active data centres with significantly improved resilience and recovery times. ICT will also look to implement infrastructure and services in such a way that operational incidents are mitigated with minimal service disruption where possible.

2.7. This however does not preclude all parts of the Council from having business continuity plans in place and tested. ICT have worked with Internal Audit and Risk Management to ensure that business continuity plans remain current and fit for purpose.

2.8. The Data Centre programme is dependent on network connectivity being in place before the migration of IT services and final decommissioning of the Sharp Data Centre. The new network design, will build in resilience, as the two new data centres will be linked and thus appear to users as one. The high-level design and tender specification was signed off by ICT architecture teams in late July. ICT will be utilising the Crown Commercial Services Framework to procure the necessary technical infrastructure, connectivity and professional services. Contracts are expected to be in place by the end of 2018.

2.9. The new core network will be delivered from both new data centres, allowing servers and applications to run out of either - underpinning the disaster recovery capability provided by the new core infrastructure and storage and backup solutions. Both new data centres are located in the Manchester area providing extremely low latency network connections. The planned network will enable flexibility with regards to the placement of infrastructure, services and applications across the two data centre facilities, allowing for proactive protection of critical services, like SAP and disaster recovery capability (quicker restoration of services).

2.10. Significant planning and discussions with business colleagues is already underway in order to help minimise operational impact. The programme team has established a Programme Steering Group, chaired by the CIO which will oversee all aspects of the programme. The Steering Group reports into the monthly ICT Board and on to Senior Management Team as appropriate.

3. Agreed Audit Recommendations

3.1. In the Outstanding Audit Recommendations report to Audit Committee July 2018 the Head of Audit and Risk Management reported that three recommendations had been outstanding for up to six months and related to ICT Disaster Recovery. These recommendations were agreed in a report issued in June 2017 and related to different elements of developing a disaster recovery plan, based on the current Sharp Data Centre.

3.2. The three recommendations not fully addressed were:

- To complete a Business Impact Assessment (BIA) of key IT services, systems and applications and agree Recovery Time Objectives / Recovery Point Objectives and specific data backup and recovery requirements (such as priorities) for each system.
- To undertake a cost / benefit exercise to identify the options around the encryption of tape based backup data.
- To ensure disaster recovery arrangements are tested on at least an annual basis, following implementation of the DR solution and creation of the DR plan.

3.3. Some actions have been taken to respond to these risks and recommendations but it is not proposed to conduct further work and allocate resources to these actions as the focus is now on completing the DC Programme rather than implement what would now be short term interim measures. ICT do have an agreed list of key ICT services and systems that would be prioritised in the event of incident or disaster and have tested DR arrangements on an ongoing basis through real incidents; including loss of service for example as was suffered during a power outage earlier this year.

3.4. The new Data Centre Programme as described above moves away from the current dependence on the Sharp Data Centre to twin active data centres. As such it is no longer considered cost effective to develop and test a full disaster recovery plan based on current arrangements and ICT consider it is appropriate to accept the risks highlighted in the audit report in advance of the proposed go-live of new arrangements.

4. PSN

4.1. The Public Services Network (PSN) is the UK government's high-performance network, which helps public sector organisations work together, reduce duplication and share resources. The PSN compliance process exists to provide the PSN community with:

- confidence the services that the Council use over the network will work without problems;
- assurance that Council data is protected; and
- the promise that if things do go wrong that the Council can quickly put it right.

4.2. PSN compliance is an ongoing process and demonstrates that the Council's security arrangements, policies and controls are sufficiently rigorous and is overseen and approved by the Cabinet Office. This programme of work is overseen by a Programme Steering Group and reports through to the ICT Board and to Senior Management Team where appropriate.

4.3. ICT report monthly to the Cabinet Office by written reports and follow up communication to maintain constant dialogue. Working in conjunction with their PSN assessor, the reporting is focused around the removal and decommissioning of all unsupported operating systems (specifically Microsoft (MS) Server 2003). There are also a number of other systems defined as 'Obsolete Platforms' that are also being decommissioned.

4.4. Following the impact of a number of high profile cyber attacks on the public sector over the past twelve months there has been a more stringent application of compliance controls by the Cabinet Office. This resulted in the Cabinet Office being unable renew the Council's PSN certification until there has been a significant reduction of dependency on MS Server 2003. The Council and Cabinet Office have continued to work collaboratively and it is noted that there has not been any operational restrictions imposed and there is no current impact for users or our partners, including DWP. This will continue so long as the Cabinet Office see regular, positive progress.

4.5. A plan and approach to strengthen current arrangements, further reduce risks and remove unsupported operating systems was developed and approved by SMT in March 2018. These arrangements include the following:

- A plan of decommissioning MS Servers and other obsolete platforms. As reported to the Cabinet Office in July there are 40 MS Server 2003 servers remaining - a decrease of 86 since March 2018. When ICT started the decommissioning exercise, 50% of the ICT estate was on old technology and this number has reduced to around 4%. The plan will reduce the total MS Server 2003 to single figures by the end of September 2018.

- Progressing a current procurement of licenses for an application patching utility that integrates with the current solution. This will address inconsistencies with patching of third party applications identified in the annual IT health check report.

- Continuing to perform health checks in the form of internal and external penetration testing by an independent third party (NCC Group). The results of these tests help highlight areas for further action as above and contribute to the submission to Cabinet Office for PSN accreditation.

- Contracting with a local third party specialist who monitors potential threats and provides on-site and remote resources that oversee the security of the ICT infrastructure.

- Creation of a new role in ICT that reports direct to the CIO. The postholder will be responsible for establishing and maintaining the enterprise vision, strategy and programme to ensure information assets and technologies are adequately protected. They will direct ICT colleagues in identifying, developing, implementing and maintaining processes to reduce risks, respond to incidents, establish appropriate standards and controls, manage security technologies, and direct the establishment and implementation of policies and procedures. Supported by a small team, this individual will regularly liaise with the Core Directorate Senior Information Risk Officer (DSIRO), Tom Powell and take over as the ICT representative at Corporate Information Assurance and Risk Group (CIARG).

4.6. The plan and approach means that ICT constantly evolves its technology and processes in line with best practice and GDPR legislation; this is important in an environment where PSN certification is achieved for the Council by ICT working to industry best practice.

4.7. ICT anticipate being able to resubmit the Council's PSN Code of Connection in November 2018.

5. Conclusion and Recommendations

5.1. Audit Committee are asked to consider the assurance provided by the update report.