AUDIT COMMITTEE **23 SEPTEMER 2021**

SUBJECT:	**IT DISASTER RECOVERY UPDATE AND ICT RECOMMENDATION PROGRESS**
DIRECTORATE:	**CHIEF EXECUTIVE AND TOWN CLERK**
REPORT AUTHOR:	**BUSINESS DEVELOPMENT AND IT MANAGER**

1. Purpose of Report

1.1 To update the committee on progress on ICT Disaster Recovery (DR) and audit recommendations for the ICT Service.

2. Background

2.1 The committee has requested an update on the ICT DR solution and outstanding audit recommendations. Both of these items have had discrete pieces of work completed and are continually reviewed and updated.

2.2 Disaster Recovery

2.3 Over a period of time the DR solution has been built up. The Council has a finite amount of resource and where possible seeks to optimise benefits from the resources available by adopting solutions that work towards resolving more than one issue.

2.4 Audit Recommendations

2.5 Due to the inherent risks associated with provision of an ICT Service, the service is required to be highly compliant with regulation and assurance from external sources. These include:

1) Internal audit reviews
2) Compliance from Central Government e.g. Public Service Network including a third party IT health check
3) Ongoing requirement to update and patch systems

2.6 This imposes a significant workload on the service and the team, and this resource is also shared with the requirement to develop and maintain the Council's infrastructure, support staff and Members and to deliver new requirements for services and needs to be balanced in terms of resourcing.

3. Progress to date

3.1 IT Disaster recovery

3.2 Several aspects have been developed which assist with the delivery of a DR solution over a number of years:

1) Backup arrangements – allowing multiple copies of data to be held within two locations on premises, and a further copy to be maintained offsite, in the 'cloud'
2) Refresh of infrastructure – a duplicate copy of the infrastructure has now been delivered which can be invoked should a disaster occur at the primary site
3) Enhanced DR copies of data – some data is not held within 'real-time' copies to reduce the likelihood of data loss should an emergency issue arise. This will reduce the amount of data that could be lost since the previous backup cycle.
4) A DR plan has been developed.

3.3 However, further work is still required in order to improve invocation times and review the DR plan to encompass any work undertaken. This is planned to happen over the next few months.

3.4 In addition, the One Council programme now meaning that more staff can work from home has improved the DR position in that staff now have devices which are remotely located, removing the likelihood of loss of desktop equipment. However, this may mean that some of the core infrastructure will need to be bolstered to provide additional resilience. Options for this are presently being considered by officers.

3.5 The DR solution is in a much improved position from previously, having multiple copies of the data, and a partial duplicate infrastructure on the secondary site, but there is more that is planned and can be done, dependent upon resource levels and risk appetite.

3.6 For example, it may not be considered necessary to have a full 'hot' failover solution, where the secondary infrastructure immediately takes over as the cost may be too high to justify. This is mitigated by critical services having Business Continuity Plans (BCP) which allow for key elements to be completed without immediate access to ICT services. BCPs are also reviewed frequently and this is planned to happen over the next year to take into account ICT DR Plans.

3.7 The level of DR will continue to be reviewed to seek opportunities for improvement.

3.8 **Audit Recommendations**

3.9 Since October 2018 there have been 5 Internal Audits, and the service has worked with the Audit team to provide assurance mapping across the range of the service. These audits have resulted in a number of recommendations, many of which are now concluded:

Audit	Date	Assurance	No. of Recs	Implemented	Outstanding
IT Applications	Oct 18	Limited	8	8	0
Malware / Anti-virus	Nov 18	Substantial	9	8	1 (Policy related)
Information Management	June 19	Substantial	16	15	1 (resourcing)
ICT Anti-Malware	Mar 20	Substantial	10	5	5 (4 policy, 1 training,
Office 365	May 21	Substantial	6 (5 not yet due)	1	1

More details on outstanding recommendations is included in Appendix A

3.10 A large proportion of the actions have been completed. One of the main areas outstanding is the review of the ICT Security Policies. A draft has been completed, and is currently being reviewed by other stakeholders.

3.11 It is intended to bring these forward to Policy Scrutiny committee later in the year and then reviewed and adopted by Executive. Some further work will need to be completed on guidance and procedures.

3.12 There have also been difficulties in resourcing over the last 18 months due to the impacts of:

1) Covid -19 response –various services and supplying services remotely
2) Furlough of staff for a period
3) Rollout of new equipment and services across the whole organisation

3.13 There are also some recommendations that will require finance to be made available in order to complete them. This is under ongoing review and will be considered alongside other pressures on the budget as part of the normal budget cycle.

3.14 **ICT Risk Register**

3.15 An ICT Risk Register has also been developed over the last year. There are currently 90 risks documented. The higher-level risks have actions in defined projects i.e. DR, which also compete for resource, or are also identified on the corporate risk register e.g. for financial and staff resources in general.

The risk register also takes account of the ICT Assurance mapping exercise which was completed in the last year, which provides an amber level of assurance overall for the ICT function.

4. Organisational Impacts

4.1 Finance – there are no direct financial impacts, although some recommendations may require additional financial resources for completion.

4.2 Legal Implications including Procurement Rules

There are no legal or procurement implications.

4.3 Equality, Diversity and Human Rights

The Public Sector Equality Duty means that the Council must consider all individuals when carrying out their day-to-day work, in shaping policy, delivering services and in relation to their own employees.

It requires that public bodies have due regard to the need to:

- Eliminate discrimination
- Advance equality of opportunity
- Foster good relations between different people when carrying out their activities

The are no Equality and Diversity issues affected by the report.

5. Risk Implications

5.1 There are some risks associated with not completing audit recommendations as they reflect good practice. However, resourcing this work can also reduce resources on other services which the Authority requires. This risk is mitigated by prioritising resources through normal ongoing management processes.

6. Recommendation

The committee is requested to review and comment on the report.

Is this a key decision?	No
Do the exempt information categories apply?	No
Does Rule 15 of the Scrutiny Procedure Rules (call-in and urgency) apply?	No
How many appendices does the report contain?	None
List of Background Papers:	None

Lead Officer: Matt Smith, Business Development and IT Manager
Telephone (01522) 873308
matt.smith@lincoln.gov.uk

Recommendations over 2 years old

Audit Area	Date	Comments / Progress	Service Area update	Revised date
Malware / Anti-virus	Nov 18	Complete revised IT Security Policy (Med)	The new IT Security Policies are in draft form and being consulted on by stakeholder across the Council. These should be complete shortly, and will then be considered for Scrutiny/Approval	December 21

Recommendations less than 2 years old

Audit Area	Date	Comments / Progress	Service Area update	Revised date
Information management	June 19	Assist Information Asset Owners to review their network drives. Update July 2021 Exploring new options for doing this. Linked to 365 migration. Extended to September 21	Since this recommendation was developed, there have been significant changes in the way files are stored through the adoption of Office 365. However, this means that there is a significant amount of work to do to review and migrate existing older files to the new environment. This will also require consultancy assistance from external suppliers to develop process/policies and for the software to be procured to manage the data. This cost is being considered against other priorities for the ICT service.	March 22 (subject to resources)
ICT Anti-Malware	Mar 20	IT security training – extended to October 21 due to license issues	New content has now been procured – officers working with supplier on delivery to users etc.	Working for October 21
		Agree minimum compliance standards for suppliers (remote access). Extended to September 2021.	This will be completed as part of the new policy framework. The new IT Security Policies are in draft form and being consulted on by stakeholder across the Council. These should be complete shortly.	December 21

		Security policy linked to mobile device management. Technical polices have been reviewed and agreed – wider written policies still being worked on. Extended September 21	The new IT Security Policies are in draft form and being consulted on by stakeholder across the Council. These should be complete shortly.	December 21
		Smartphones and Tablets - review the (security) policy. Technical polices have been reviewed and agreed – wider written policies still being worked. Extended to September 2021	The new IT Security Policies are in draft form and being consulted on by stakeholder across the Council. These should be complete shortly.	December 21
		Complete a briefing note/guidance and training for other IT officers relating to Alien Vault – reviewing AlienVault suitability – request for additional funding for other types of cyber Protection – being reviewed by BDITM extended to September 21	This software is no longer in operation. The ICT team are using different tools to monitor the threat. These are partially implemented with additional controls being developed. As these tools are implemented, further guidance will be developed	March 22
		Review and update the Incident management policy/procedure - Extended September 2021	The new IT Security Policies are in draft form and being consulted on by stakeholder across the Council. These should be complete shortly. In addition, the ICT DR plan is being reviewed in the light of new investment in the service over the next few months.	December 21

Office 365	May 21	Updating the project plan list and reporting to Technology Board as well as change logs/lessons learned logs	The Technology group are update monthly on progress. The Organisational Change Lead also updates CMT on a regular basis	Report to Technology Board by December 21 on project outcomes
		Considering whether the migration of data from existing network files to 365 should be treated as a separate project - to be discussed with Board	This project is referred to above – it is likely to be dealt with as a separate project now that the rollout of devices is coming towards a conclusion. However, this project requires resources to be identified both in terms of a significant amount of financial resource which is currently being considered and staff time which will impact across the authority. For this reason during Covid this has not been seen as a high priority project.	To be determined when resources allow
		Update the project risk register and report into Board periodically	The Technology group are update monthly on progress. The Organisational Change Lead also updates CMT on a regular basis	Report to Technology Board by December on project outcomes
		Formally report financial spend for licences, hardware, and other project expenditure to the Board (discussed currently)	The Technology group are update monthly on progress. The Organisational Change Lead also updates CMT on a regular basis	Report to Technology Board by December on project outcomes
		The DPIA has been finalised and the EHRA will be finalised shortly	The Technology group are update monthly on progress. The Organisational Change Lead also updates CMT on a regular basis	Complete
		Day to day operational procedures will be completed	Resources have been diverted onto the rollout of new devices	Aiming to complete by October 21