AUDIT AND RISK MANAGEMENT COMMITTEE
12 JUNE 2017

REPORT TITLE:	**DIGITAL UPDATE**
REPORT OF:	**HEAD OF DIGITAL & SENIOR INFORMATION RISK OWNER (SIRO)**

REPORT SUMMARY

This report provides Members with a progress update on actions taken by Digital Officers to remove and mitigate risk associated with underinvestment in IT infrastructure in the past.

RECOMMENDATION

Members should note the report.

SUPPORTING INFORMATION

1.0 REASON FOR RECOMMENDATION

1.1 The former Head of Digital and Senior Information Risk Owner (SIRO), Mike Zammit, gave a verbal report to members in January.

1.2 At the March meeting members requested a written report and a senior member of Digital to attend the June meeting.

1.3 In April Mike Zammit left the authority. The interim Head of Digital is Jeff Ashworth, the interim SIRO is Surjit Tour.

2.0 OTHER OPTIONS CONSIDERED

2.1 No other options considered.

3.0 BACKGROUND

3.1 At the meeting of this Committee in January 2017, Mike Zammit, the then Head of Digital and SIRO gave a verbal report on the following programmes of work:-
IT Contingency.
Disaster Recovery.
Data Loss Prevention.
Cyber Security.
Information Governance.

3.2 This written report will document and update Mike Zammit's verbal report on the 5 programmes of work. The work will now be split between the interim Head of Digital and interim SIRO.

PROGRESS

3.4 IT Contingency and Disaster Recovery

3.5 The fibre ring serving council buildings in central Birkenhead has been upgraded, including improved resilience, to provide a link to the Merseytravel datacentre.

3.6 The tendering process for the migration of all production services to the Merseytravel datacentre and the repurposing of the Treasury building datacentre as a Disaster Recovery site has been completed and was won by SCC.

3.7 The project with SCC will start week commencing 5 June with the initial phase, the discovery and design phase, estimated to last 6 weeks.

3.8 Please find Project Plan attached in Appendix A

3.8 **Data Loss Prevention (DLP)**

3.9 The Council has a number of technical and procedural controls to reduce the deliberate or accidental loss of sensitive information. These include: policies and documented procedures; training of staff; endpoint protection (eg laptop encryption; anti-virus and anti-malware software); and disabling of Universal Serial Bus (USB) ports.

3.10 Three DLP recommendations from Internal Audit are still outstanding. One relates directly to the creation of a policy and will be completed alongside implementation of the General Data Protection Regulation (GDPR) compliance project. Completion of the other two recommendations, which relate to technical controls and the Information Asset Owners' responsibility to enforce appropriate working practices, will follow on from the identification of the information assets. This will also be part of the GDPR compliance project.

3.11 Five DLP recommendations from the Information Commissioner's Office (ICO) audit are still outstanding. Two will be completed by end of May 17. Two have been superseded by superior solutions that are currently being implemented. One recommendation is awaiting contact and agreement from a 3rd party.

3.12 **Cyber security**

3.13 Of the five medium priority recommendations, the two infrastructure recommendations (firewalls and wireless access) are in progress. The information governance recommendations have been covered as part of the ICO audit.

3.14 Work by Digital to replace all XP machines with Window 7 machines has significantly reduced the site's vulnerability to malware/ransomware attack.

3.15 Digital's implementation of McAfee's software security suite enabled Digital to install an additional security package to detect the 'wannacry' malware within hours of the Ransomware attack on 12th May.

3.16 As part of Wirral's Target Operating Environment project, Windows 2003 servers were upgraded to Windows 2008 or 2012. This has increased the site's security

3.15 **Information governance (IG)**

3.16 All IG policy and procedure documents are being reviewed following recommendations made in the ICO Audit and the Internal Audit review of Intranet Policies and Guidance. A rolling programme of reviews has been planned to address all of the recommendations made in these audits, including ensuring that all documents are up-to-date, are in a standard format, have nominated owners and a scheduled review cycle. The review programme has been scheduled to complete in March 2018 to coincide with the Council's readiness for GDPR compliance.

4.0 FINANCIAL

4.1 Budget has been allocated for the data centre move.

5.0 LEGAL IMPLICATIONS

5.1 There are none arising from this report.

6.0 RESOURCE IMPLICATIONS

6.1 There is none arising from this report.

7.0 RELEVANT RISKS

7.1 There is a risk to IT resilience until the completion of the data centre move.

8.0 ENGAGEMENT/CONSULTATION

8.1 None

9.0 EQUALITY IMPLICATIONS

9.1 There are none arising from this report.

REPORT AUTHOR: Jeff Ashworth
Head of Digital
telephone: 0151 666 3079
email: jeffashworth@wirral.gov.uk

SUBJECT HISTORY (last 3 years)

Council Meeting	Date
Audit and Risk Management Committee	Jan/March 2017