AUDIT AND RISK MANAGEMENT COMMITTEE

26 OCTOBER 2022

REPORT TITLE:	**ICT CONTINUITY CONTROLS**
REPORT OF:	**DIRECTOR OF RESOURCES**

REPORT SUMMARY

This report has been prepared in response to a request by the Chair of the Audit and Risk Management to provide an update on the resiliency of Wirral Council’s IT infrastructure.

RECOMMENDATION

The Audit and Risk Management Committee is recommended to note the report.

SUPPORTING INFORMATION

1 REASON FOR RECOMMENDATION

1.1 To provide Members of the Audit & Risk Management Committee with an opportunity to review the resiliency of the Council's IT Infrastructure and the continuity plans in place.

2 OTHER OPTIONS CONSIDERED

2.1 The report is provided for information purposes in response to a direct request by the Chair of the Audit & Risk Management Committee, and as such no other options have been considered.

3 BACKGROUND INFORMATION

3.1 IT resilience means being prepared for any type of planned or unplanned disruption or disaster, and the ability to mitigate the risk of downtime allowing the organisation to continue working. IT resilience is an essential part of business resilience.

3.2 Planned disruption can include maintenance and upgrades of systems or hardware, move to cloud technology, datacentre changes, integrations. Unplanned disruption can include infrastructure or hardware failures, natural disasters, security breaches, ransomware, or user error.

3.3 As services are transformed, there is increasing dependence on digital technologies to deliver these. This leads to an increased risk of being disrupted by cyber-attacks and security breaches.

3.4 Business Continuity is used to proactively implement policies, processes, and activities that ensure the smooth running of critical systems during and after a disruption. This includes the identification of risk and management of this, creation of business continuity plans, and validation and testing of processes and procedures.

3.5 Disaster Recovery is the act of putting systems, data, and networks back to a previous state after a disruption or disaster has occurred. The disaster recovery plan focuses on the infrastructure and sets out the operational IT recovery processes following disruption, this includes the provision of alternative sites, data backup and offsite replication, and robust servers, storage, and networking.

3.6 There are 4 stages to Business Continuity and Disaster Recovery:

- Stage 1: Prevention
    - Mitigation of the risk
- Stage 2: Preparedness
    - Planning for the disruption
- Stage 3: Response
    - Developing plans detailing actions for responding to a disruption.

- Stage 4: Recovery
    - Developing plans detailing the recovery process following a disruption.

3.7 Where applications are delivered via Software as a Service (SaaS) the management of the application and underlying infrastructure is delivered by the supplier. The IT role moves to monitoring and audit and ensuring that contracts include appropriate terms and deliverables around security, backup, and recovery options.

Prevention

3.8 The Prevention stage is about mitigating the risk of unplanned disruptions.

3.9 The risk is mitigated by ensuring suitable measures are in place are the different layers of the IT environment:

- Client devices: Computers, mobile phones, tablets
- Network: Firewalls, routers, switches
- Storage
- Servers: Windows, Unix, Linux
- Applications

3.10 McAfee endpoint security solution is installed on computers and servers to protect against viruses and cyber-attacks.

3.11 Security update processes are in place to ensure client devices, storage, servers, and network devices are kept up to date.

3.12 A third party provides 24*7 monitoring of the Council's Firewalls. The Firewall is the equivalent of the front door into the IT infrastructure.

3.13 Cyber security training to provided to all Council staff to help prevent unplanned disruptions.

3.14 Key IT staff have undertaken Certified Information Systems Security Professional (CISSP) training. This training is focussed on developing IT security skills and knowledge.

3.15 Regular engagements take place with the National Cyber Security Centre (NCSC) to help monitor and secure networks and websites.

Preparedness

3.16 The Preparedness stage is about having processes in place to mitigate the impact of any disruption to services.

3.17 The Council has two datacentres, one located in the Treasury Building in Hamilton Square, and one located in Mersey Travels datacentre in Georges Dock in Liverpool.

3.18 The datacentres are setup as a Primary and Secondary datacentre, with the Primary datacentre being in Liverpool.

3.19 Replication technology is used to replicate data between the two datacentres. This ensures that a second copy of data is available should the primary datacentre not be available.

3.20 An automated system is in place that would automatically bring up business critical applications in the secondary datacentre should the primary datacentre not be available.

3.21 A manual process is in place to bring all other applications online in the secondary datacentre should the primary datacentre not be available.

3.22 All applications have been classified as to their criticality and impact should they not be available. The classification covers prioritisation levels 1 – 5 from applications that have life and death implications, to critical systems such as our financial systems, to business-critical systems such as those that would have customer facing impact, to non-critical or lower priority applications.

3.23 Any applications classified as level 1 or 2 are covered by the automated system for bringing online in the secondary datacentre.

3.24 A backup solution is in place to backup data to a third location, using a virtual vault off the Council network. The ‘vault’ protects data from cyber-attacks using an immutable file system that cannot be modified, deleted, or encrypted by hackers.

3.25 The backup solution provides an air gap away from the Council network meaning that if required, data could be restored to a third location if both the primary and secondary datacentres were not available.

Response and Recovery

3.26 Business Continuity and Disaster Recovery Plans are currently being refreshed to reflect the increasing adoption of Software as a Service (SaaS) for business applications.

3.27 As part of the refresh of the Business Continuity and Disaster Recovery Plans, the Recovery Time Objectives (RTO) and the Recovery Point Objectives (RPO) will be reviewed for each application.

3.28 RTO is the amount of time after an outage that an application needs to be recovered. RPO is the amount of data that can be lost for an application following an outage.

3.29 Following the refresh of the Business Continuity and Disaster Recovery Plans, a scenario will be chosen to test the response to a Cyber Security attack.

4 FINANCIAL IMPLICATIONS

4.1 There are no financial implications arising as a direct result of this report.

5 LEGAL IMPLICATIONS

5.1 There are no financial implications arising as a direct result of this report.

6 RESOURCE IMPLICATIONS: STAFFING, ICT AND ASSETS

6.1 There are no resource implications arising as a direct result of this report.

7 RELEVANT RISKS

7.1 All risks associated with the IT resilience are captured within either the Information, Digital Programme or ICT risk register.

8 ENGAGEMENT/CONSULTATION

8.1 There is no member engagement as a direct result of this report.

9 EQUALITY IMPLICATIONS

9.1 There are no equality implications arising as a direct result of this report.

10 ENVIRONMENT AND CLIMATE IMPLICATIONS

10.1 There are no environment or climate implications as a direct result of this report.

11 COMMUNITY WEALTH IMPLICATIONS

11.1 There are no community wealth implications as a direct result of this report.

REPORT AUTHOR: PETER MOULTON
0151 666 3868
petermoulton@wirral.gov.uk

APPENDICES

None

BACKGROUND PAPERS

ICT Business Continuity Plans

Information Governance Risk Register

ICT Departmental Risk Register

Digital Programme Risk Register

SUBJECT HISTORY (last 3 years)

Council Meeting	Date