

AUDIT COMMITTEE - 4 DECEMBER 2018

PART I – DELEGATED

9. CYBER SECURITY: AGED SERVER ESTATE

1 Summary

1.1 At the September 2018 Audit Committee, the ICT Section Head made a request for a further extension for the following outstanding Cyber Security audit recommendation:

- All devices that are running unsupported operating systems should be upgraded to run operating systems that are supported by the developer.
- Where it is not possible to upgrade the operating system of a device, it must be isolated from the Councils' IT network and appropriate security controls implemented.

1.2 As part of a wider Core Infrastructure Transformation programme, this work stream had several stages; server review, dependency identification, agree plan and deliver.

1.3 Each of the out of support servers followed either a decommission path, upgrade path or migration into a more secure part of the network, termed "Walled Garden". The current position of the 29 unsupported servers as of mid-November 2018:

- 5 have been migrated to the "Walled Garden"
- 15 have been decommissioned
- 9 servers require further action and have a scheduled decommission or migration date prior to the end of December 2018

2 Details

2.1 Securing Unsupported Operating Systems

2.1.1 All Operating systems require updates, through the form of patching, in order to secure the devices from emerging threats. In addition to this, as with other software, vendors have software cycles and upgrade paths where required in order improve performance, security, provide additional features etc.

2.1.2 At the start of the Core Infrastructure Transformation the W3R estate had a number of unsupported Microsoft operating systems. This meant that Microsoft stopped providing those essential security updates those servers needed, therefore making those devices more vulnerable to attacks from the outside world.

2.1.3 Through the Core Infrastructure Transformation programme, we have decommissioned over 160 servers across the estate. Several months ago we identified 29 servers, with an unsupported operating system that could not be easily decommissioned as there were dependencies on other infrastructure projects. For example the Exchange (Email servers), which were unsupported can only be decommissioned upon the successful completion of the W3R Active Directory and Exchange user migration project.

- 2.1.4 In order to secure the network the “Walled Garden” was created and the migration programme was initiated.
- 2.1.5 The “Walled Garden” is a term given to the part of a network that has additional security layers, thereby securing devices that are more prone to attack. Network access is enabled through a firewall, meaning that internal network traffic restricted from both sides. The “Walled Garden” segregates traffic from our internal network, where our other supported servers reside.

2.2 Current Position

- 2.2.1 Migration of services and servers to the “Walled Garden” or to be decommissioning requires extensive investigation and understanding of dependencies, or else the risk is loss of services to business users. The need for the extension to resolve this project is as a result of some of those investigations taking longer than expected.
- 2.2.2 To date 5 servers have been migrated to the “Walled Garden”. A further 15 were decommissioned as a result of other projects concluding and resources focussed in this area.
- 2.2.3 Our current position is there are 9 servers awaiting migration and/or decommission which we are confident will be resolved by 31 December 2018.

3 Options and Reasons for Recommendations

- 3.1 No recommendation, report is for noting.

4 Policy/Budget Reference and Implications

- 4.1 The contents of this report are within the Council's agreed policy and budgets.

5 Financial Implications

- 5.1 The recommendations of this report are within the Council's agreed policy and budgets.

6 Legal Implications

- 6.1 None.

7 Equal Opportunities Implications

- 7.1 Relevance Test

Has a relevance test been completed for Equality Impact?	No – there is no change in service as a result of this recommendation.
--	--

8 Customer Services Centre Implications

- 8.1 None.

9 Risk Management and Health & Safety Implications

- 9.1 The Council has agreed its risk management strategy which can be found on the website at <http://www.threerivers.gov.uk>. In addition, the risks of the proposals in the report have also been assessed against the Council's duties under Health and Safety legislation relating to employees, visitors and persons affected by our operations. The risk management implications of this report are detailed below.
- 9.2 The subject of this report is covered by the ICT service plan(s). Any risks resulting from this report will be included in the risk register and, if necessary, managed within this/these plan(s).
- 9.3 There are no risks to the Council in agreeing the recommendation(s).

The following table gives the risks that would exist if the recommendation is rejected, together with a scored assessment of their impact and likelihood:

Description of Risk		Impact	Likelihood
1	Failure to identify all server related dependencies, results in a loss of service.	4	1

- 9.4 Of the risks detailed above none is already managed within a service plan.
- 9.5 The above risks are plotted on the matrix below depending on the scored assessments of impact and likelihood, detailed definitions of which are included in the risk management strategy. The Council has determined its aversion to risk and is prepared to tolerate risks where the combination of impact and likelihood are plotted in the shaded area of the matrix. The remaining risks require a treatment plan.

Likelihood	A						Impact	Likelihood
	B						V = Catastrophic	A = >98%
	C						IV = Critical	B = 75% - 97%
	D						III = Significant	C = 50% - 74%
	E						II = Marginal	D = 25% - 49%
	F						I = Negligible	E = 3% - 24%
		I	II	III	IV	V		F = <2%
Impact								

- 9.6 In the officers' opinion none of the new risks above, were they to come about, would seriously prejudice the achievement of the Strategic Plan and are therefore operational risks. The effectiveness of treatment plans is reviewed by the Audit Committee annually.

10 Recommendation

- 10.1 No recommendation, the report is for noting.

Report prepared by: (Emma Tiernan, ICT Section Head)

Data Quality

Data sources:

None

Data checked by:

Not applicable

Data rating:

1	Poor	
2	Sufficient	√
3	High	

Background Papers

None

APPENDICES / ATTACHMENTS

None