Assessor
for Central Scotland

Agenda Item 7

Title:	**Update Report on IT Audit**
Meeting:	**Central Scotland Valuation Joint Board**
Date:	**16 November 2018**
Submitted By:	**Assessor & ERO**

Central Scotland Valuation Joint Board

1. Purpose of Report

1.1 At its meeting on 29 June 2018 the Board was advised of the outcome of planned internal audit review of IT issues. The Board noted that report and requested that it be updated on the progress to meet the recommendations contained within the internal audit report.

1.2 This report provides an update on the progress that has been made to implement those recommendations

2. Recommendation(s)

2.1 The Board is asked to consider and comment on the progress made to date.

3. Background

3.1 The Board approved a planned programme of internal audits for 2017/18 at its meeting on 29th September 2017. That planned programme included an audit of the Board's IT security measures. The audit was subsequently carried out and gave substantial assurance as to the IT measures in place. It did list eleven recommended actions that should be taken. These were agreed by the relevant mangers.

3.2 The results of the audit were reported to the Board at its meeting on 29 June 2018. The Board noted the outcome of the audit and asked to be kept informed as to the progress with implementing the recommendations. It was agreed that a progress report should be supplied to the Board at its meeting on 16 November 2018.

4. Progress

4.1 This section shows in tabular form the eleven recommendations and the progress that has been made

No.	Recommendation	Progress
1	Written policies and procedures should be prepared setting out • Overarching corporate IT security arrangements including responsibilities for enforcing all security policies • Processes for requesting and authorising access to the network and key IT systems and • the approach for recovering data back-ups and/or all IT services in the event of a system failure, corruption or disaster	• The overarching security policy is currently being drafted • Processes for requesting and authorising access are in place • Written procedures are in place documenting the approach for recovering data backups and IT services
2	All IT security policies and procedures should be reviewed and updated on an annual basis.	All policies and procedures have been reviewed and updated with the exception of the Electronic Communications policy. This policy requires an extensive rewrite and work is ongoing.
3	The Corporate Risk Register should be amended to include the risks associated with outsourcing IT services.	Risk Register is currently being updated to reflect risks associated with outsourced IT services.
4	The server room should be kept in a clean and tidy condition, with appropriate cable management practices adopted.	Completed.
5	The Uninterruptible Power Supply (UPS) system should be tested and maintained on a quarterly basis, with a record kept of all tests undertaken.	Completed.
6	Annual assurances should be sought from suppliers in relation to the security measures which have been adopted to safeguard all externally hosted hardware and software (and the data thereon)	Assurances have been sought and responses are being received.
7	The IT Asset Register should be updated to include all tablet devices issued to the Operational Management Team and the owner and location of all other IT assets.	Completed
8	Access Request Forms should be developed for each IT system setting out the user profiles which may be requested. Thereafter user accounts should only be created or modified by Systems Administrators on receipt of a	Completed

	fully completed and authorised request form, with a copy of the form retained to support all system users.	
9	Timescales for the review, testing and deployment of security patches, updates and service packs should be reduced.	Patching policy has been updated to reduce the timescales and is in line with National Cyber Security Centre recommendations.
10	A register of all software updates should be established and maintained. The register should set out: the nature of each update: all testing undertaken (including outcomes): and the Officer responsible for authorising its upload to the ‘live’ environment	Register has been established and is being maintained.
11	An IT Asset Disposal Register should be established and maintained. This register should set out the date of disposal, method of disposal, and provide a link to the corresponding certificate of destruction where applicable.	Register has been established and is being maintained.

5. Consultation

5.1 No consultations have been carried out.

6. Implications

Financial

6.1 The recommendations have been carried out with no financial impact to the Board

7. Resources

7.1 The increasing levels of monitoring and recording of activities, does have a staff resource implication. In the light of the increasing IT security demands we have expanded our IT Team to include the post of Technical Support Officer. That post holder will assist our Systems Administrator in testing, recording and monitoring of all IT security administration amongst other duties.

8. Legal

8.1 There are no legal implications arising from this report

9. Risk

9.1 By implementing these recommendations the risk to the Board has been mitigated. However given the ever changing IT security threat there will always be a residual risk to the Board.

10. Equalities

10.1 No Equality Impact Assessment was required as part of this report.

11. Sustainability/Environmental Impact

1.1 No Sustainability Impact Assessment was required as part of this report.

12. Conclusions

12.1 Work has taken place to implement the recommendations the majority of which have been fully implemented with the remainder being in progress.

____
Assessor

Author – Pete Wildman, Assessor 01786 892212
Date:

Appendices

None

List of Background Papers:

The following papers were relied on in the preparation of this report in terms of the Local Government (Scotland) Act 1973:

- None