Audit Improvement Plan Activities

Audit Improvement Plan Activities

KEY FOR RECOMMENDATION PRIORITY

Priority 1	- Findings that are fundamental to the integrity of the Service's business processes and require the immediate attention of management.
Priority 2	- Important findings that need to be resolved by management.
Priority 3	- Findings that require attention.

Cyber Security (Data Backup) – Head of Corporate Support

Main Recommendations	Priority	Management Response	Implementation Plan	Management Update	Progress
1. The ICT team maintain a system backup and recovery spreadsheet which captures key information regarding what is backed up, where it is backed up, who is responsible, backup frequency, retention period and recovery details. The document lists four systems which are maintained by third-party contractors, however none of these contained any information in relation to the areas listed above. Two of the four systems were identified by the Network & Security Manager as critical, with the other two non-critical. The critical systems were discussed in further detail with the Head of ICT, who was able to evidence that backup requirements and expectations are outlined within contractual documentation between the parties.	3	Action agreed and steps already in place to obtain the back-up data for the critical control systems (BOSS and Vision). Other third-party systems will also be added to the data we hold on internal systems.	**Recommendation/Corrective Action:** To receive periodic updates from third-party contractors and partners on backup and recovery results. To ensure that the system backup and recovery spreadsheet is updated in relation to the third-party back-up arrangements in place, supporting the oversight and awareness within the ICT team. **Responsibility:** Head of ICT **Target Date:** 30 September 2023	Work is ongoing with the NFSP to obtain regular system backup updates. A recovery log is in place to record completed backups.	On Track

They also stated that they work closely with the Network Fire Service Partnership (NFSP), who provide these critical systems. It was, however, agreed that the Service should be more proactive in seeking periodic evidence of the backups performed by the NFSP, as per the requirements within the contracts. It should also be ensured that the system backup and recovery spreadsheet is updated to include complete information on the third-party arrangements in place.					