INDEPENDENT AUDIT COMMITTEE **AGENDA ITEM NO: 14**
19 December 2013

ASSET MANAGEMENT

Purpose

1. This paper informs the committee of action which has taken place on Asset Management since the last meeting. This is in response to the No Assurance report received in August 2013 which was reported to this committee in September.

Background

2. The Finance Department currently maintain Wiltshire Police's Asset Management Register (Hardcat). The register holds information on assets with a significant value or is attractive to theft. A 12 month rolling programme is in place which results in all locations being visited by the Finance Department recording the assets which are held in each room. The main category of asset held on the system is ICT assets.

3. In recent years the Force has implemented the following processes with the aim to increase the assurance level to reasonable;

    - Launched a communications campaign to raise awareness
    - Ensured posters are produced and circulated across the Force
    - Documented Policy and Procedure, available on Firstpoint for all the Force
    - Cleaned up the system to remove minor assets
    - Produced and implemented a 12 month plan of visits and reports
    - Discussed outcomes as part of the quarterly budget monitoring meetings

4. It was expected that all these positive steps would achieve an increase in assurance level however the August audit identified weaknesses in activity and a requirement for ICT to improve there processes surrounding the handling of assets.

The Audit Report

5. The Internal Audit report is attached. This has been updated to show actions taken by management in the recent months and where the Force is in resolving the issues.

6. Overall some good progress has been made in most areas with ICT now taking a more responsible role in the management of assets.

Matters of Concern

7. When carrying out the audit 2 main concerns were identified;

    - The possibility of theft of ICT assets
    - The possibility that data has been lost

8. In completing the work the Head of Business, Transformation and Change (the Department Head for ICT) has been reviewing the situation and regularly meeting with staff. His general view is that no significant fraud has taken place.

9. The issue of lost data is more complex. The Force currently issue 2 mobile assets which hold data: Laptops and USB Memory Sticks.

10. As mentioned in the response to the audit report the Force are currently requesting all identified owners of laptops to confirm that they remain the holder of the asset. This process is expected to be complete by the end of the year. The Asset Management System does however hold 76 laptops which are not allocated to individuals. A Force wide email has been sent requesting staff to identify all laptops in there vicinity including 'office' laptops. This is expected to identify the majority of laptops however as some of these laptops date back to 2000 I do expect there to be a number of unresolved assets. The Force will then have to take a view on whether these assets have been disposed of but not recorded or whether further investigation is required.

11. The majority of laptops issued by the Force are dumb, not allowing data to be saved on the hard drive. Therefore to access data they would firstly need to obtain access through the normal laptop log on, they would then need to access force systems with a specific account and password. This limits the risk considerably.

12. However some users have requested that data be allowed to be kept on the hard drive to allow them to use applications and save data when not in a Wi-Fi enabled area. This reduces security, allowing access to data as soon as the initial laptop sign on screen has been passed. Unfortunately ICT have no record of the laptops they have enabled to save data on the hard drive. There is a risk therefore that a minority of the laptops being written off may contain data.

13. The Force has allocated 276 USB Memory Sticks. These memory sticks require passwords to access the data. 216 of these are allocated to named individuals. No confirmation has ever been requested that the individuals still hold the memory stick. Included within the list of holders are a number of officers who have left the Force. Action has started to confirm with holders that they continue to hold the memory stick.

14. The remaining 60 are not allocated to individuals and require investigation.

15. The possible loss of data assets is a big concern to both the Chief Constable and the PCC. The issue has been raised with the Force Security Manager. His response is below;

'Regardless of whether a device is encrypted or not, unless we are able to evidence to the contrary, we must presume that the devices had stored on them, personal data or otherwise sensitive information (Protectively Marked). In the case of unencrypted devices, the presumption then is that the information / data may have been compromised as a consequence of loss and or poor accounting / control. In the case of encrypted devices, then no such presumption can be made as, by definition, the information / data is inaccessible because of the installed encryption (a valid statement only when we can be assured that the 'password' hasn't been written down and held with the device)'

16. Based on the volume of assets which are unallocated the likelihood of loss is high. Based on this the Security Manager <u>will</u> have to notify the Office of the Information Commissioner and the National Police Information Risk Management Team at the Home Office immediately.

17. Whilst the response from the Information Commissioner is unknown it is likely that they will investigate the position. They will expect a firm, timely action plan to be put in place. Depending on their views a fine may be exercised.

Proposed Action Plan

18. The following plan was agreed at the Commissioners Monitoring Board on 9 December;

    a) A Force wide communication ordering that ALL non Wiltshire Council Laptop be returned to ICT for validation (and where possible replaced with Wiltshire Council Laptops)

    b) The order that ALL memory sticks should be returned to ICT. Where required policy documents should be loaded directly on to the Council Laptops.

19. At the end of January the position will be reviewed, post the orders, with the aim that in the first week of February a decision is made by the Chief Constable and PCC whether to write off data assets which have not been traced in the knowledge that the Information Commissioner will require this data.

20. This process will be managed by the Deputy Chief Constable as part of a Gold Group.

Wiltshire Council Laptops

21. There is concern that the Force will run into similar problems with the Council Laptops. This is unlikely as the solution provided is encrypted and based on laptops that can be 'killed' remotely if lost or allocation is unknown. The solution can also identify which user is using the specific laptop. On allocation the user is asked to sign for the laptop. As data can be saved on the laptops no requirement for memory sticks exists.

Risks

22. The risk of data loss is identified earlier in the report and is significant.

23. There is financial risk concerning any fines the Information Commissioner may apply. There is also the reputational risk surrounding the possible loss of data. This is high and requires some proactive communications to be produced.

Conclusion

24. The board is asked to note the response to the audit and that a number of laptops and memory stick require investigation.

25. The board should also note the probable report to the Information Commissioner concerning the unallocated assets (the Chief Financial Officer will update the committee of the latest position at the committee meeting) and that the Deputy Chief Constable will manage the issue in the ICT Gold Group.

Clive Barker
Chief Finance Officer to the Chief Constable and PCC