Report to the Finance & Performance Management Cabinet Committee

Report Reference: FPM-017-2010/11

Date of meeting: 22 November 2010

Epping Forest District Council

Portfolio: **Legal & Estates.**

Subject: **Verification of Audit Logs.**

Responsible Officer: **David Newton**   **(01992 564580).**

Democratic Services Officer: **Gary Woodhall**   **(01992 564470).**

Recommendations/Decisions Required:

That, in view of the existing compensating controls, separate access violation logs should not be purchased.

Executive Summary:

The latest audit, carried out in April 2010, identified weaknesses in controls in the monitoring of Access Violation Logs resulting in a finding of 'Limited Assurance'. The audit results were discussed at the Audit & Governance Committee in June 2010 and ICT agreed to carry out further research and assist service application administrators in compliance.

Having conducted further research and evaluated existing compensating controls, it is not felt appropriate to invest the funds that would be required to address what is felt to be a relatively minor risk.

Reasons for Proposed Decision:

This report identifies that it is not possible to produce system specific violation logs without incurring large expense to the Council and that recent developments in technology have significantly reduced the risk of access violation.

Other Options for Action:

Pay third party suppliers to develop bespoke solutions, but this will be extremely expensive.

Report:

1.   ICT have approached all suppliers of the 13 core systems. None can offer satisfactory solutions to the production of access violation logs. None of the suppliers had plans to include access violations logs in future releases, but were willing to investigate the possibility on a bespoke basis. The average costing was £10,000 per system, a total of £130,000.

2.   The audit identified that violation logs produced by ICT from the Active Directory **(AD)** system**,** which controls access to the Councils' Local Area Network **(LAN)** were fully compliant. AD is a Microsoft product, is recognised industry standard and very secure. **All**

users must be successfully authenticated by this system before they can access ANY application held on the LAN. Most modern systems, for example, Information at Work, no longer require separate system logins but rely solely on the AD system. This is the trend for most newly developed systems and highlights the confidence the IT industry has in the AD product.

3.   ICT does not have access to the source code of any of the 13 core systems included in this audit. It is therefore not possible to adapt any of these systems in-house. Extensive research into third party monitoring software has also failed to identify a suitable alternative solution

4.   Compensating controls are also in place. The Council is connected to the Government's secure extranet **(GCSx)**. A very strict code of connectivity **(CoCo)** makes access to the Councils' LAN extremely secure. For example AD enforces complex passwords; there is substantial physical security for access to both servers and workstations and also policies enforcing best practice.

5.   To summarise, it is not technically possible to comply with this audit requirement without considerable cost to the Council. The AD product and other controls, make the LAN extremely secure and the risk of any system access violation minimal. The Chief Internal Auditor has been kept advised of these developments.

Resource Implications:

If separate system access violation logs are to be purchased the cost would be £130,000. There are no spare funds in the Capital Programme so either a supplementary estimate would be required or a scheme that is currently planned would have to be abandoned.

The implementation of system access violation logs on 13 separate systems would require a substantial amount of staff resource, which would result in delays to other projects.

Legal and Governance Implications:

None.

Safer, Cleaner and Greener Implications:

None.

Consultation Undertaken:

Liaison with suppliers and software suppliers.

The Chief Internal Auditor has also been consulted and made the following comment:

Regular meetings have been held between the Assistant Director of Finance and the Chief Internal Auditor in assessing the cost of various solutions, existing compensating controls and the level of outstanding risk. As a result of these discussions, the Chief Internal Auditor has reassessed and reduced the risk level applied to the follow up audit in the 2010/2011 audit plan.

Background Papers:

Verification of Audit Logs – Follow up Audit – April 2010
Audit & Governance Committee in June 2010

Impact Assessments:

Risk Management
It is felt that the existing compensating controls are adequate and that the risk associated with not having separate system access violation logs is not significant.

Equality and Diversity:

Did the initial assessment of the proposals contained in this report for relevance to the Council's general equality duties, reveal any potentially adverse equality implications?   No

Where equality implications were identified through the initial assessment process, has a formal Equality Impact Assessment been undertaken?   No

What equality implications were identified through the Equality Impact Assessment process?
None

How have the equality implications identified through the Equality Impact Assessment been addressed in this report in order to avoid discrimination against any particular group?
N/A