AGENDA ITEM NO. 9

BRISTOL CITY COUNCIL

Audit Committee

11th November 2011

Report of: Strategic Director (Corporate Services)

Title: Update on the take up of online Information Security training

Ward: N/A

Officer Presenting Report: Manager, Information Management

Contact Telephone Number: 0117 922 3119

RECOMMENDATION

That the Audit Committee notes the information in the report.

Summary

This report includes;
Update on the Information Security Risk in the Corporate Risk Register
Update on take up and future plans for Information Security Training
Response to the Grant Thornton interim audit report recommendation
Update on Penetration testing.

The significant issues in the report are:

We have assessed the overall Information Security risk to the authority and will be taking a recommendation to the Corporate Risk Group in early February 2012 to revise the level of risk to AMBER.

We have refined the definition of the risk to key areas identified in this process. These risks have clear mitigation plans assigned to further reduce the level of risk.

It is not cost effective to implement the external Audit recommendation to implement Intrusion Detection and Intrusion Preventions systems.

Policy

- The council's Information Security policy is available at http://intranet.bcc.lan/ccm/navigation/policy-and-procedures/information-management/information-security/.

Consultation

- **Internal**

  Plans to improve security are agreed by IMTSG (Information Management Technology Steering Group).

- **External**

  Security plans and standards conform to external recommendations, in in particular those the central government authority on Information Assurance, CESG – http://www.cesg.gov.uk/).

Context

Information Security Risk to the authority has been assessed and the key risks identified. We now have a clear set of mitigation plans which will inform the proposed new Corporate Risk Register entry.

- As a result of the review of the Corporate Risk entry, we will be recommending that the level of risk be reduced to AMBER. We will be taking the revised Corporate Risk entry and mitigation plans to the Corporate Risk Group in early February 2012.

Information Security Training

- We have now trained over 90% of staff. We will be delivering refresher training on an annual basis to all staff. The refresher training will be launched in December 2011.

- Security awareness training for new starters has been embedded into the Corporate Induction process. As of August 2011 all new starters will complete their security awareness training as part of their induction process.

Grant Thornton interim report Recommendation.

- The Grant Thornton report recommended that Bristol implement an Intrusion Detection / Intrusion Prevention system to supplement existing protection from the BCC Firewalls.

- Intrusion Detection / Prevention system is estimated to cost £100,000. In addition to this are ongoing support and management costs.

- We have no other requirement mandating implementation Intrusion Detection at this point. We are not mandated to implement this in order to connect to GCSX.

- Financial systems will be reviewed 2012/2013 and therefore we will work closely with the project to ensure any new systems are delivered to meet security requirements.

- In view of these points, we are not recommending that Bristol pursue the implementation of IDS/IPS. We have written to Will Godfrey and Peter Robinson to confirm their approval of this way forward.

- Penetration Testing - main issues identified were password quality and strength , SMTP configuration improvement, patching updates. We have taken action to address these issues, and are using this service on an annual basis as part of our ongoing assurance processes.

Proposal

- Audit Committee are asked to note the information in this report.

Other Options Considered

- None relevant

Risk Assessment

- Information Security remains at Red on the Corporate Risk Register. The actions reported here will continue to mitigate that risk.

Equalities Impact Assessment

- Not relevant

Legal and Resource Implications

Legal

None sought

Financial

The work described in the report is being undertaken within existing budgets.

Land

Not Applicable

Personnel

Potential for disciplinary proceeding against individual members of staff.

Appendices:

None

LOCAL GOVERNMENT (ACCESS TO INFORMATION) ACT 1985
Background Papers:

None