AGENDA ITEM NO. 14

BRISTOL CITY COUNCIL

Audit Committee

28th June 2013

Report of: Strategic Director (Corporate Services)

Title: Update on Information Security

Ward: N/A

Officer Presenting Report: Information Security Manager

Contact Telephone Number: 0117 903 6927

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 the development of the Information Security Strategy.
Update on future plans for Information Security Training
Update on the Information Asset Owners

The significant issues in the report are:

We assessed the overall Information Security risk to the authority and recommended to the Corporate Risk Group in February 2012 to revise the level of risk down to AMBER. The level of risk remains at AMBER.

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 particular those the central government authority on Information Assurance, CESG – http://www.cesg.gov.uk/).

Context

Audit committee last received a report in November 2012. There were four key strands to mitigation activities; security strategy, security training, secure E-mail and Information Asset Owners.

Members asked for an update report which is set out below.

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 have revised the level of risk downwards to AMBER. The risk remains at AMBER.*

Information Security Strategy

We have developed an approach, focused on key activities and delivery methods. Much of this work will take place as part of the various change programmes which are shaping business change across the authority.

Please refer to Appendix A - Information Security Strategic Action Plan Delivery Proposals April 2013

Information Security Training
Annual refresher training was delivered last year. We are now into a regular annual delivery programme. Planning for further training to be delivered from the E-Learning portal is in progress.

Secure E-mail For Non Government bodies and Members of the Public
A facility to enable simple, but secure E-mail communication between the authority and non government bodies e.g. the voluntary sector and members of the public is now in pilot. This facility will provide a secure and efficient communication channel to citizens and partners. It will also improve our environmental efficiencies.

Information Asset Owners
Four existing employees have been identified to undertake the role of an Information Asset Owner for the following information areas.

- Customer data
- Finance data
- Property
- HR

We have used the information needs of the major change programmes to prioritise these information areas.

Key responsibilities of this role include:

- Setting data quality standards
- Authorisation of Information Sharing Protocols
- Driving the strategic re-use of information

Other change programmes and replacement of IT systems will continue drive this piece of work.

Proposal

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

Other Options Considered

- None relevant

Risk Assessment

- Information Security remains at Amber 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 proceedings against individual members of staff.

Appendices:

Information Security Strategic Action Plan Delivery Proposals April 2013

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

None

APPENDIX (14) A

Information Security Strategic Action Plan – Delivery Proposals

April 2013

The Information Security Strategy was outlined in draft in August 2012. This paper sets out ideas on how changes in the organisation impact the original draft, and how the various elements can be approached.

Principles

We will adopt a number of key principles:

- Actively balance security risk against business risk
- Acknowledge that information security breaches may occur (there is never zero risk), and plan to minimise their impact
- Make individual responsibilities clear, and hold people to account
- Build information security into our culture
- Support suppliers and partners to meet our security needs

Strategic Objectives

- The council is able to take advantage of new technologies and working methods while keeping personal and confidential data safe and maintaining legal compliance
- A balanced approach to overall risk is reflected by an information security risk at AMBER or below
- Numbers of information security incidents are held at an agreed levels
- External suppliers and delivery partners understand and can deliver on the council's security requirements
- Council managers and staff understand their security responsibilities, can meet them and are held to account for doing so

Proposals for delivering the action plan:

Change/Action	*Delivery method*
Risk Management: Develop our capacity to manage risk, and establish an agreed appetite for risk • Work with strategic managers and the risk management group to establish coherent methods of managing risk and an agreed overall risk appetite • Work with all change programmes to assess information security risk as part of their overall planning	Short term: • IM Team support change projects and programmes to assess security risk as part of overall risk planning • Security team & Risk Management Group publish guidance Medium-long term: • "Strategic & Support deal" within Future Council Operating Model work to address risk appetite more broadly
Policies & Culture: Establish individual responsibility • Update and simplify the existing security policy • Make information security planning and assurance an inherent part of all change • Work with the Bristol Workplace programme to develop staff security guidelines alongside changes to working practices • Identify and clearly label confidential information • Establish owners with clearly defined responsibilities for all council information • Educate and engage with staff so that good practice becomes part of normal working practice	Short term: • Security team & IMTSG appoint key Information Asset Owners • Annual refresh of security training for all staff • IM Team support change projects and programmes to assess security risk as part of overall risk planning Medium-long term: • People programme to implement common basic skills framework for all staff • Security Policy review within Strategic & Support "policy bonfire" framework • Bristol Workplace programme to produce guidelines for day-to-day working practice
Suppliers and delivery partners: Ensure that suppliers understand and deliver the council's security requirements • Work with the emerging Strategic Commissioning programme to include information security in commissioned service specifications and contracts • Work with local economic and market development initiatives	Short term: • Security Team provide ICT Sourcing strategy with material to support engagement with local suppliers • Security risk assessments for commissioning activity through the Project & Programme framework.

to ensure that our requirements are clear and deliverable • Work with commissioners to establish the right security requirements for the services they commission	Medium-long term: • Strategic Commissioning programme to include Information Security elements in market development and commissioning process standards strands
Information Sharing: Establish an effective and comprehensive set of information sharing agreements with our partners and suppliers • Agree standards for sharing agreements and their management • Establish and make available a supply of expertise in writing sharing agreements • Establish formal ownership of all sharing agreements	Short term: • Security team & IMTSG appoint key Information Asset Owners • IMSTG agree a one-council framework for internal sharing • IM Team catalogue and manage existing sharing agreements Medium-long term: • IM Team to develop city-wide sharing framework(s) within the partnership that emerges from the City Deal, Future Cities demonstrator and other partnering initiatives
Technology: Use technology to secure information where cost effective • Provide easy-to-use facilities for council staff to handle information safely • Implement technical standards for council-managed IT in areas such as encryption, separation of data etc • Establish testable technical and management standards for technology suppliers and partners • Embed security testing of both internal and external systems and services	Short term: • IM Team support change projects and programmes to assess security risk as part of overall risk planning • Security team and IMTSG agree technology security standards (including testing regimes) Medium-long term: • Technology and Bristol Workplace programmes deliver secure facilities as needed for new ways of working

Implication:

We need to ensure that the following programmes include appropriate work to delivery Security Strategy elements:

- Bristol Workplace
- People
- Technology
- ICT sourcing
- Once council TOM/Strategic & Support services
- Strategic Commissioning

Other programmes and project will also need to work to information planning, risk assessment and technical standards.