Scrutiny Report

Overview and Scrutiny Management Committee

Part 1

Date: 15 November 2018

Subject Annual Information Risk Report 2017/18

Author Scrutiny Adviser

The following people have been invited to attend for this item:

Invitee:	Area / Role / Subject
Rhys Cornwall	**Head of People and Business Change**
Mark Bleazard	**Information Development Manager**

Section A – Committee Guidance and Recommendations

1 Recommendations to the Committee

The Committee is asked to consider the Annual Information Risk Report 2017/18 attached as **Appendix 1** and provide comments for consideration by the Cabinet Member.

2 Context

Background

2.1 Local Authorities collect, store, process, share and dispose of a vast amount of information in accordance with their duties under the Data Protection Act and other legislation. The Council must meet its statutory responsibilities effectively and protect the personal information it holds throughout its life cycle; from creation through storage; use, retention, archiving and deletion. The principle of using and securing data is outlined in the Digital Strategy.

2.2 The Information Commissioner's Office (ICO) currently has the power to fine organisations up to £500,000 for data breaches to ensure organisations take this responsibility seriously. In May 2018, the EU General Data Protection Regulation enables much higher fines of 20 Million Euros or 4% of turnover.

2.3 The purpose of the Council's Annual Information Risk Report is to provide an assessment of the information governance arrangements for the Council as outlined in the Information Risk Management Policy and identify where further action is required to address weaknesses and make improvements.

2.4 The actions outlined in the attached report form part of the People and Business Change Service Plan further detail incorporated in the Digital and Information Team Annual Business Plan. Information risk is also considered in the Corporate Risk Management Strategy and Register.

2.5 The Overview and Scrutiny Management Committee has this opportunity to comment on the draft Annual Information Risk Report and the Council's information governance arrangements.

3 Information Submitted to the Committee

Appendix 1 – Annual Information Risk Report 2017-18

4. Suggested Areas of Focus

Role of the Committee

The role of the Committee in considering the report is to consider:

- The robustness of control measures and management arrangements;
- The Reduction in the number of incidents and not of major significance, the lowest number recorded in the five year period since the risk report has been produced and no incidents reported to the Information Commissioner's Office this year;
- Resilience of action to remedy incidents such as the ransomware attack this year and previous breaches;
- The Action plan included for on-going compliance and protection for the future and whether the planned actions are sufficient to mitigate any risks identified.

Section B – Supporting Information

5 Supporting Information

5.1 The 2016 -17 Annual Information Risk Report was presented to Scrutiny Committee on 26 July 2017 by the Head of People and Business Change when it was explained that it was not a mandatory report required by Regulators but good practice and provide scrutiny the opportunity to see how the Council was managing information .

The Committee raised the following issues:

- The Committee requested the figures on how many staff in all areas of the Council have been on / scheduled to undertake training, and were advised that 699 have been trained corporately. The Committee were advised that there was a comprehensive action plan for Social Services with a bespoke training for staff, and that this would be prioritised.
- Members discussed the use of Egress; and Members were advised that training was in progress.

- Councillor attendance at training was discussed, and the Committee were advised that there had been two training sessions with 32 Councillors having attended in total. It was noted that further training sessions could be arranged if requested. The Committee queried whether the outcomes of learning from training sessions were tested, and were advised that this was not done as a matter of course for any internal training sessions.

- Members queried whether there was evidence of Local Authorities being specifically targeted for cybercrimes, and if there have been any fines given for data breaches. It was unclear if these attacks were at random or if they were co-ordinated, from email addresses being cloned. Officers also advised that the Authority was in a good position following the attack last year, and assured Members that the Council was taking appropriate preventative measures, but that the key was not to be complacent.

- With regard to securing information when sending via email, Members were advised that Egress was the system used by the Council. Other Authorities were using systems such as drop box to share sensitive information without using the email system.

- In relation to data management, there was no reference within the report to how data is reproduced from obsolete technology, and whether there was a method to audit this data.

- Members asked who was responsible for school data. Members were advised that Education are responsible for their own data, that training was offered and delivered where needed, however there were not sufficient resources to provide direct support.

- In relation data on old technology, data was migrated from older system to the newer system, with the majority of paper files are either converted electronically or archived. There were also regulations governing how long certain data needed to be kept for, Members agreed that this information should be contained within the report.

- More serious threats, such a terrorism and ransomware were discussed. The Head of People and Business change advised that all IT staff were certificated in data protection and that the Council was reasonably confident on its current position, although again it was highlighted that the key was not to become complacent. Terrorism hacking risks were a reasonably low risk, as Council's were not high targets in the wider context in terms of the value of the information that could be obtained. Random, untargeted attacks were easier to defend against, and the Authority was in as good a position as others to prevent these sorts of breaches.

- Business continuity in the event of cyber-attacks was discussed, with specific mention to how Education would fare with them being on a separate network. Members were advised that worst case scenario would be similar to what happened with the Council last year with the breach, whereby within hours the virus was isolated, networks were closed down with everything on the networking being recoverable from the previous days back up. Members were also advised that tests are routinely carried out by high tech companies against day to day threats, and at least once a year IT have a health check to try to find vulnerabilities with networks.

- In relation to improvements to existing infrastructure and the migration of backups from tape to disk, it was clarified that this would be implemented over a number of months and that data replication will be tested.

- Members queried how the establishment of Shared Resources Service (SRS) had impacted on the information risk, and were advised that the main difference was the Blaenavon Offices were more set up for modern IT systems making it more secure, compared with Civic Offices. A disaster recovery system is being looked into which would further reduce risk.

6 Links to Council Policies and Priorities

- The Council's Information Risk Management Policy sets out the Council's approach to information risk management including roles and responsibilities. The policy also details the processes in place to manage information risks effectively, including the Annual Information Risk Report.

The Digital Strategy, approved by Cabinet October 2015 sets the overall direction for the management of information, and information governance is also considered in the Annual Governance Statement produced for the inclusion in the Council's Annual Statement of Accounts and reported to Audit Committee.

The Annual Information Risk report has strong links to the modernising Council supporting function which supports the Corporate Plan Commitments and Well-being Objectives;

Well-being Objectives	Promote economic growth and regeneration whilst protecting the environment	Improve skills, educational outcomes & employment opportunities	Enable people to be healthy, independent & resilient	Build cohesive & sustainable communities
Corporate Plan Commitments	Thriving City	Aspirational People		Resilient Communities
Supporting Function	Modernised Council			

7 Wellbeing of Future Generation (Wales) Act

5 Ways of Working

- Does the report demonstrate how as an authority we are working in accordance with the sustainable development principles from the act:
  - ***Long Term***

    The importance of balancing short-term needs with the need to safeguard the ability to also meet long-term needs
  - ***Prevention***

    How acting to prevent problems occurring or getting worse may help public bodies meet their objectives
  - ***Integration***

    Considering how the public body's well-being objectives may impact upon each of the well-being goals, on their other objectives, or on the objectives of other public bodies
  - ***Collaboration***

    Acting in collaboration with any other person (or different parts of the body itself) that could help the body to meet its well-being objectives
  - ***Involvement***

    The importance of involving people with an interest in achieving the well-being goals, and ensuring that those people reflect the diversity of the area which the body serves.

8. Background Papers

- Overview and Scrutiny Management Committee – 26 July 2018
- Digital Strategy 2015 - 2020
- The Essentials - Wellbeing of Future Generation Act (Wales)
- Corporate Plan 2017-2022

Report Completed: November 2018