Report

Community Planning & Development Scrutiny Committee

Part 1

Date: 10 June 2015

Item No: 5

Subject **Annual Information Risk Report 2014-15**

Purpose To provide the Scrutiny Committee with the opportunity to comment on the draft Annual Information Risk Report 2014/2015 and the Council's information governance arrangements.

Author Information Development Manager
Overview & Scrutiny Officer

Ward General

Summary Local Authorities collect, store, process, share and dispose of a vast amount of information. The Council must meet its statutory responsibilities effectively and protect the personal information it holds throughout its life cycle; from creation through storage; uses, retention, archiving and deletion, as outlined in the Information and Technology Strategy.

The purpose of this, the council's third Annual Information Risk Report, is to provide an assessment of the information governance arrangements for the Council and identify where further action is required to address weaknesses and make improvements.

Proposal **The Committee is requested to consider the Annual Information Risk Report 2014-15 and provide comments for consideration by the Cabinet Member**

Action by Information Development Manager
Information Governance Manager

Timetable As reported

This report was prepared after consultation with:

- Head of Law and Regulation – Monitoring Officer
- Head of Finance – Chief Financial Officer
- Head of People and Business Change
- Chief Internal Auditor
- Information Governance Group

Background

The purpose of this report is to provide an assessment of the information governance arrangements for the council and identify where action is required to address weaknesses and make improvements. The benefits of this report are as follows:-

- Provide an overview of the council's information governance arrangements;
- Highlight the importance of information governance to the organisation and the risks faced;
- By establishing a baseline, the report will enable comparison of performance in future years;
- Identify and address weaknesses and develop an action plan;
- Reduce the risk of failing to protect personal data and suffering any subsequent reputational and financial penalties (the Information Commissioners Office can issue a fine of up to £500,000 for data breaches).

Financial Summary

There is no specific cost associated with the report. Any costs incurred would be normal costs associated with the running of the service. However, the report is designed to highlight risks and to reduce potential penalties from the Information Commissioner's Office (ICO) if information is not managed correctly.

Risks

A huge amount of information is held by the organisation. This needs to be managed appropriately. Further details of risks are provided in the report and those identified below represent some high level risks.

Risk	Impact of Risk if it occurs* (H/M/L)	Probability of risk occurring (H/M/L)	What is the Council doing or what has it done to avoid the risk or reduce its effect	Who is responsible for dealing with the risk?
Data breach results in fine imposed by the Information Commissioner's Office or reputational damage	H	L	All the actions detailed in this report are designed to mitigate this risk.	Information Governance Manager (IGM) in conjunction with Information Management team
Council is unable to make best use of, and share the data it holds due to a lack of confidence in the integrity and security of the information.	L	H	Information management development, staff communications and Records Management policy	IGM

* Taking account of proposed mitigation measures

Information Risk is also incorporated into the Corporate Risk Register, as outlined in this report.

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 IT and Information Strategy sets the overall direction for Information Management and governance arrangements, 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 actions outlined in this report form part of the Customer Services and Digital Innovation service improvement plan.

Options Available

1. **Do nothing**
2. **Note the annual information risk report and provide comments for consideration by the Cabinet Member.**

Preferred Option and Why

The preferred option is option 2 – Note the Annual Information Risk Report 2014/15 and provide comments for consideration by the Cabinet Member. This will provide an understanding of the current position in relation to information governance and give an opportunity to monitor progress on actions identified

Comments of Chief Financial Officer

There are no direct financial implications within this report and the strength of the controls should minimise the potential of any significant financial fines from the Information Commissioner.

Comments of Monitoring Officer

There are no specific legal issues arising from the Report. The Annual Information Risk Report confirms that the Council has in place robust information governance arrangements and security policies to meet its statutory obligations under the Data Protection Act, PSN accreditation and information sharing protocols. There have been no significant security breaches within the last 12 months involving a reference to the ICO.

Staffing Implications: Comments of Head of People and Business Change

There are no staffing implications associated with this report.

Information Risk Management is now included in the Corporate Risk Register. The Annual Information Risk Report includes details of the management of the Information Risk Register and significantly high risks will be escalated accordingly.

Consultation

Comments of the Chief Internal Auditor

Having sound information governance arrangements in place strengthens the overall corporate governance arrangements for the Council. This report clearly demonstrates the Council has appropriate and effective arrangements in place for information governance and deals with further improvements in a transparent and inclusive way in order to minimise the likelihood of significant financial fines.

The Information Governance Group were also consulted on the report, and comments included in the final version.

Background Papers

Information Risk Management Policy (reviewed December 2014).
Annual Information Risk Report 13/14
Annual Governance Statement 14/15
Corporate Risk Management Strategy and Register (updated May 2015)

Dated: 12th May 2015

Annual Information Risk Report 2014/15

Created by	Information Governance
Date	12/05/2015
Reviewed by	
Date	

Document Control

Version	Date	Author	Notes / changes
V0.1	20/04/15	Tariq Slaoui	Initial draft based on previous report
V0.2	29/04/15	Mark Bleazard	Updated draft
V0.3	05/05/15	Tracy McKim	Updated draft with Scrutiny requirements
V0.4	11/05/15	Mark Bleazard	Updated draft for Info. Governance group
V0.5	20/05/15	Mark Bleazard	Updated with consultee comments
V0.6	1/06/2015	Tariq Slaoui	Updated following briefing meeting

Table of Contents

Contents

Executive Summary **1**

1. Background and Purpose **3**

1.1. Purpose of the Report and Benefits *3*

2. Current Position **3**

2.1. Accreditation and Audit *4*
Public Services Network (PSN) compliance (formerly GCSx) 4
Payment Card Industry Data Security Standards (PCI-DSS) 4
Wales Audit Office (WAO) 4

2.2. Information Governance Culture and Organisation *6*
Information Governance Culture 6
Organisation 7

2.3. Communications and Awareness Raising *7*
Staff Guidance 7
Training Courses 8
Information Policy Development 13

2.4. Information Risk Register *14*

2.5. Security Incidents *14*

2.6. Information Sharing *15*

2.7. Business Continuity *16*

2.8. Technology Solutions *16*

2.9. Records Management *18*

2.10. Freedom of Information and Subject Access Requests *18*

3. Risk Management and Associated Action Plan **19**

3.1. Risk Management *19*

3.2 Action Plan *21*

Executive Summary

The council has a statutory requirement to look after the data it holds. **The Information Commissioner's Office (ICO) has the power to fine organisations up to £500,000 for data breaches to ensure organisations take this responsibility seriously.**

This is the third Annual Information Risk Report which provides an assessment of the information governance arrangements for the Council as outlined in the Information Risk Management Policy. The report highlights:

- Accreditation and audit
    - The successful re-accreditation to the Public Services Network (PSN) represents a good achievement for the council. The change of compliance regime provides more flexibility and local management of risk.
    - Payment Card Industry data security standards (PCI-DSS), formally compliant in 2014/15 for the first time
    - Continued scrutiny from the Wales Audit Office provides a valuable external viewpoint for making improvements. The information governance review will result in specific actions
- Information Governance Culture and Organisation
    - The Information Governance Group continues to play an important and effective role in the strategic management of information risks
    - As part of the Welsh Audit Office review, focus groups were held to establish employee understanding of Information governance
    - The information security incident reporting policy has been simplified, improved and communicated to staff
- Communications and awareness raising:
    - Guidance continues to be provided to staff with particular emphasis this year on risks as a result of the NATO summit held in Newport
    - The on-going staff training programme continues to be an important part of the council's information governance arrangements
        - First ever formal training courses provided for schools
        - Significant increase in those attending corporate training course compared with previous years
        - Slight reduction in attendance within Social Services compared with last year
        - Tailored workshop training has been developed in conjunction with the Contact Centre
    - Development of the records management policy
    - Existing policies reviewed and reminders communicated where appropriate.
- Information Risk Register
    - Information risk register developed as identified in previous year's information risk management policy
    - Information risk register managed by Information Management team and monitored by the Information Governance Group
    - High level information risks included in the corporate risk register for the first time and more joined-up process with the corporate risk register
- Security Incidents
    - Consistent numbers of information security incidents over the last three years
    - Most incidents relatively minor
    - No incidents reported to the Information Commissioner's Office (ICO)
    - Two most significant incidents in Social Services
    - Improvements made to Civic Centre access
    - Improved information security incident reporting policy as detailed above

- Information Sharing
    - New Information Sharing Protocols developed for Newport Drug & Alcohol Service, Multi Agency Risk Assessment Conference (MARAC) and Not in Education, Employment or Training (NEET)
    - Current and future developments for POVA, Provider Services, Team around the Cluster, Anti-Social behaviour, crime and disorder, Flying Start
- Business Continuity
    - Priority IT systems agreed for the first time by the council
    - Previous action plan being progressed with work to complete
    - Address issues raised by Wales Audit Office (WAO)
- Technology Solutions
    - Most significant development is the implementation of Egress solution for secure and large file transfer
    - Other solutions remain to maintain information security, supported by PSN compliance
    - Microsoft Forefront Identity Management (FIM) solution under development
    - Consideration of the move to cloud storage where appropriate including appropriate controls
    - Wales Audit Office annually review the controls applied to key financial systems (reported to Audit Committee)
- Records Management
    - Implementation of electronic document management on-going
    - Modern Records facility for paper archive documents created at Civic Centre
    - Approximately 40% complete with more documents to move and record on the IT system
    - Records Management policy developed
- Freedom of information and Subject Access Requests
    - There are risks when publishing responses which need to be managed.
    - The number of freedom of information requests has increased
    - A future development is the proactive publication of data as part of the openness and transparency agenda
    - A review of processes around Subject Access Requests has started with further work required
- Risk Management and Associated Action Plan
    - A number of risks have been identified in this report and associated actions planned as outlined in section 3.2 with further detail being developed in the Information Management team's business plan. Actions are under the following areas:
        - Staff and councillor awareness
        - PSN Accreditation and improved information governance
        - PCI accreditation
        - Technical Solutions
        - Information Sharing
        - Business Continuity
        - New projects

1. Background and Purpose

As a local authority we collect, store, process, share and dispose of a vast amount of information as part of our duties. 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. This is outlined in the Information and Technology Strategy.

The actions outlined in this report form part of the Customer Services and Digital Innovation service plan and further detail will be incorporated in the Information Management team's business plan. Information Risk is also considered in the Corporate Risk Management Strategy and Register (January 2015 update).

1.1. Purpose of the Report and Benefits

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

The purpose of this report is to provide an assessment of the information governance arrangements for the council and identify where action is required to address weaknesses and make improvements.

The benefits of this report are as follows:-

- Provide an overview of the council's information governance arrangements;
- Highlight the importance of information governance to the organisation and the risks faced;
- Where relevant this report will compare performance with previous years and with the aim of continuous improvement;
- Identify and address weaknesses and develop an action plan;
- Reduce the risk of failing to protect personal data and any subsequent reputational and financial penalties (the Information Commissioners Office can issue a fine of up to £500,000 for data breaches).
- Ensure that appropriate risks are escalated to the Corporate Risk Register.

This is the third Annual Information Risk Report and covers the period Apr 14-Mar 15.

2. Current Position

This part of the report identifies the council's current position in relation to information governance; this includes a number of external compliance requirements. For the 2014/15 year additional activities were undertaken to address the risks presented by the 2014 NATO summit held in Newport.

2.1. Accreditation and Audit

The council is subject to accreditation to the Public Services Network (PSN) which replaces the GCSx (Government Connect Secure Extranet) accreditation previously held. The council is also required to comply with the PCI-DSS Payment Card Industry Data Security Standards when it handles card payments for customers. In addition the council is subject to audit from the Wales Audit Office to ensure appropriate information governance is in place.

Public Services Network (PSN) compliance (formerly GCSx)

The council's PSN compliance was originally due to expire on 23rd September 2014 but this was extended by the Cabinet Office until 23rd April 2015. The council's PSN submission was made using new beta guidance in March 2015. The council was notified of successful compliance in early April 2015. A significant amount of work was required for this successful accreditation by IT and Information Management.

The Cabinet Office adopted an amended approach this year which provides more flexibility for organisations. The Cabinet Office now enables organisations to consider their own approach to risks. This does not actually change the fundamental requirements but places more responsibility on individual organisations. The risk of non-compliance within the required period would result in the Council being denied access to key systems such as the Customer Information System CIS from the Department for Work and Pensions (DWP) which is used by Housing Benefits.

It appears that the new compliance regime will be less restrictive around 'Bring Your Own Device' BYOD technology. The current project for member BYOD, and any extension for staff use will need to be assessed as part of the compliance review.

Payment Card Industry Data Security Standards (PCI-DSS)

In December 2014 the council completed a Self-Assessment Questionnaire (SAQ) for Payments Card Industry (PCI) data security standards and was successful in meeting the requirements of the standard. This required additional technical measures to be taken and processes to be amended in some cases. Security scans are carried out quarterly to ensure card data is secure when it is transmitted across the internet to the council's payment providers.

This is the first time the council has achieved PCI compliance which is an important validation of its card handling technology and processes. Reaccreditation is required to comply with the latest version of the standard (version 3). It is expected that further work will be required to achieve the requirements of this amended standard.

Wales Audit Office (WAO)

The Wales Audit Office (WAO) carries out audits annually which involve IT and Information Management. In 2014 WAO completed a review of Information Governance and the final report has now been received. The review included interviews with key officers, including the Senior Information Risk Owner (SIRO), attendance at the Information Governance Group, focus groups with service managers and staff, interview with the cabinet member, an extensive document review and a detailed review of a number of security incidents.

Key messages from the draft report on information governance are:-

(6) The Council has a good record of responding to information security breaches and of reporting these, where appropriate, to the Information Commissioner's Office (ICO).

The Council staff we spoke to felt confident and empowered to report breaches, but they are not always clear on:

- *the official method of reporting information security breaches;*
- *to whom in the Customer and Information Service they should report breaches; or*
- *who is the Senior Information Risk Owner (SIRO).*

(7) Currently, one officer of the Council holds three roles of:

- *Head of Customer and Information Service – to provide strategic direction for delivery of ICT;*
- *Senior Information Risk Owner for the Council – to take overall ownership of the Council's Information Risk Policy; and*
- *Chair of the Information Governance Group – that includes the requirement to scrutinise actions on the annual risk report and responses to information security incidents.*

(8) The combination of one person holding these three roles creates a conflict of interest in that one person oversees both service delivery and scrutiny of that service delivery. The Council has acknowledged the conflict of interest inherent in this situation and has given an undertaking to make alternative arrangements.

(9) The Council has information security training arrangements in place and staff who have attended this training have found it informative and useful.

(10) The Council has still not tested business continuity plans and does not know if it would be able to maintain critical services in the event of a catastrophic failure of its critical IT systems. The Council should test its information technology business continuity plan to ensure it operates as anticipated. In particular it should test a scenario where both server rooms at the Civic Centre are not available to determine how long it will take to set up an offsite server room and what effect this has on its timetable for restoring its critical systems.

(11) As part of the 'New Ways of Working' programme, the Council is rolling out an Electronic Records Management System (EDRMS) project and has set up a new Modern Records. The Council plans to complete the deployment of EDRMS across all services by March 2016 with all active paper records stored in the system. However, the Council has not completed an overall assessment of all of its information data sources and has not yet appointed data owners. Without these in place, it will be difficult to achieve the full EDMS project objectives.

The progress outlined in the review, including staff awareness and training is helpful. A number of the actions have been progressed since the review was completed, this includes work on the reporting of security incidents, improved communications and clear links to the corporate risk register. PSN compliance for 2015 has also now been achieved.

The requirement to change the chair of the Information Governance Group is being considered. This group meets quarterly and has continued to meet since the review, with regular reports to the Deputy Leader.

The development of Information Asset Owners is a priority for 2015/16.The Information Governance Group convenes on a quarterly basis. It draws representation from across the Council with a brief of scrutinising information security.

The terms of reference of the group, and role of the Senior Information Risk Owner (SIRO) are now published on the Council's Intranet. Progress over the past year includes – deployment of Egress product and a full review of incident reporting.

The process for reporting incidents has now been reviewed to ensure that all incidents are reported promptly. This is also outlined on the Intranet and has been highlighted in staff news bulletins.

As outlined in the review significant progress has been made in the rollout of EDMS and this work is on-going. The development of Information Asset Owners is also referenced in this report.

Further developments are required for business continuity and these are referenced in this report.

2.2. Information Governance Culture and Organisation

The council's information governance arrangements have improved over a number of years commencing with the requirements of the Government Secure Extranet (GCSx) and then the increased requirements of the Public Services Network (PSN). The change to a more flexible regime in relation to PSN compliance will arguably mean that the council's information governance arrangements will be even more important in future.

The council created its Information Governance Group in November 2013. This group meets quarterly and has been a major improvement in the council's information governance.

Information Governance Culture

Last year's report (2013/14) included analysis of a questionnaire developed to understand the organisation's information governance culture. This identified good overall awareness of information security requirements by staff. Some concerns were raised over public access to buildings, especially the Civic Centre which resulted in an action identified for 2014/15. As a result additional security has been provided on specific entrances at the Civic Centre which now provides consistent levels of security. The 2013/14 survey also identified the need for formal training to be provided and the training section details the council's continued commitment to this. The survey also highlighted that many staff do not know the correct procedure to follow in the event of an incident. This has been addressed by an amended incident reporting policy including a simplified notification form and communication of the amended policy.

As part of the WAO review, focus groups with managers, and employees looked at the organisation's awareness of information security. As outlined in the previous section, this work identified that staff felt confident and empowered to report breaches. The review suggested the need to improve incident reporting awareness and communication of the incident reporting policy which has now been addressed.

Intranet pages and advice on information governance has also been developed this year and it is proposed to survey employees in the new year to continue to evaluate developments.

Organisation

The council has a named Senior Information Risk Owner (SIRO) role that is responsible for information security within the organisation; this role is part of the role of the Head of Customer Services and Digital Innovation. The day to day operational work is carried out by the Information Management team and IT.

An important aim of this report is to ensure that members are aware of the information security responsibilities of the council and to enable guidance to be provided. The annual risk report represents a useful opportunity for the Scrutiny Committee for Community Planning and Development to comment and make suggestions for scrutiny of the past year's performance and improvements going forward.

The Information Governance Group has met quarterly since its inception in November 2013 chaired by the Head of Customer Services and Digital Innovation. These quarterly meetings enable strategic information governance issues to be discussed as well as monitoring progress of actions identified in this report. The group is made up of representatives from different services and notably this includes Audit representation linked to the council's wider governance arrangements and risk management. As detailed above, the Wales Audit Office suggested amending the chair of the Information Governance Group.

The next step in embedding information governance in the organisation is the development of Information Asset Owners that have responsibility for the information held in their service.
Schools are their own "data controllers" as defined in the Data Protection Act so each school is responsible for its own information governance. The council recognises that it has an important role to play supporting schools to meet their obligations and this is provided by the Education service and Information Management working together. Four information security sessions for schools were run in June 2014 and this is detailed in the schools training section below. This is the first specific information security training provided for the council's schools. This will be supplemented by further training planned for 2015/16. A review of information security policies relevant to schools has commenced and further work is required during 2015/16.

2.3. Communications and Awareness Raising

Employees play a key role in information governance and it is important for them to understand legal requirements and best practice. This can be driven by awareness-raising (staff bulletin articles, leaflets etc.) together with training to enforce key messages.

Staff Guidance

A number of reminders on good practice have been provided in the weekly staff bulletin and intranet and these continue to be regular and varied. The focus of staff communications this year has been around general security awareness, including specific requirements for the NATO event and how to log security incidents. Following the WAO review in 2014 the role of the Information Governance Group and SIRO has been communicated to all staff and publicised on the Council's intranet.

The content of this advice continues to be recorded by the Information Management team to evidence the messages communicated to employees. An information security leaflet is provided to all staff that attend training and also other staff as necessary. The team regularly assess information from the Information Commissioner's Office (ICO) to ensure that key messages are communicated to employees. This is especially significant in the case of fines issued by the ICO to other organisations.

Training Courses

A number of different information security courses are run. These courses have an amount of common content but also include tailored content depending on the specific course. The content is also updated to provide relevant and up-to-date examples. The courses run are:-

- Social Services courses
- Corporate courses
- Councillor courses
- Schools courses
- Ad hoc courses and presentations

These training courses demonstrate the council's continued commitment to information security. Training is valuable when analysing security incidents and is a major consideration if incidents are reported to the Information Commissioner's Office (ICO).This highlights the value to the council of this work. There has been significantly increased attendance on corporate training with a small decrease in attendance in Social Services course. Course feedback as detailed below is consistently good.

Social Services Courses

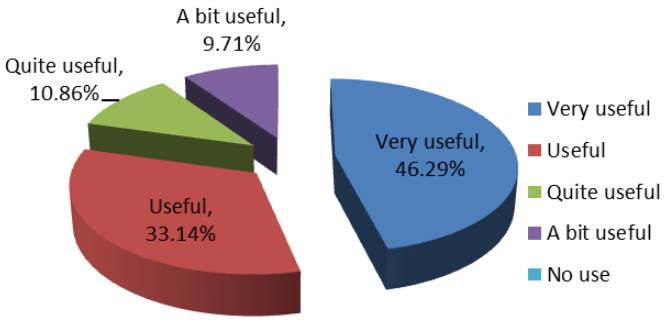
Social Services employees represent a high risk group due to the nature of their business and the information they handle as part of their roles. Specific Social Services training courses commenced in April 2013. This is more detailed and specific to Social Services staff. The part one course is a tailored version of the corporate training course aimed at Social Work and administrative staff.

In 2014/15 the number of staff attending the part one course was 182 which is less than in 2013/14 when attendance was 226. This, in part, reflects less staff that require training, but also reflects slightly fewer courses being run.

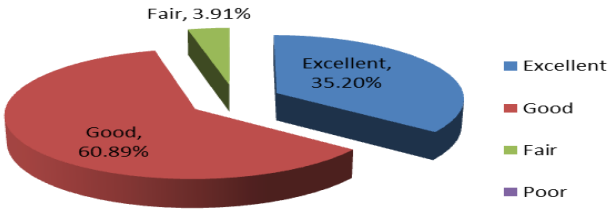
The part two course provides more detail on information sharing and subject access requests including what information should be redacted (removed) from subject access requests to ensure inappropriate information is not disclosed. This course is being reviewed to ensure it is relevant. Consequently the number of staff attending was 16 in 2014/15 compared with 62 in 2013/14.

Feedback from staff attending courses is gathered for each training course held. Feedback gathered has generally been positive and this is demonstrated by some analysis below:-

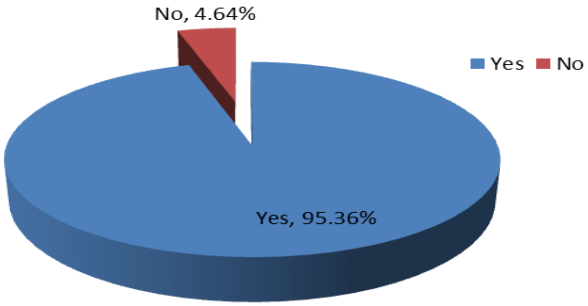
How useful has this training been for the work that you do?



Overall I considered the training to be?



Would you recommend that other colleagues attend this training?



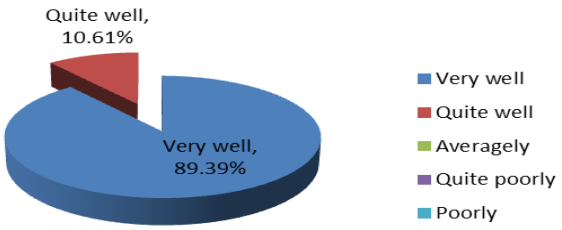
Corporate Courses

These are scheduled on a monthly basis with a maximum of 15 attendees. The content had minor updates in 2014/15 to ensure continued relevance and up to date content.

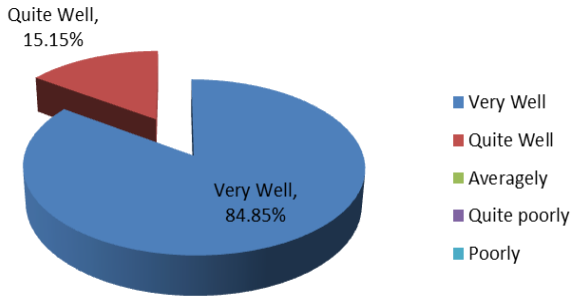
In 2014/15 the number of staff attending the corporate course was 152 compared with 92 in 2013/14 and 57 for 2012/13. This continued improvement in attendance was due to a concerted effort to raise awareness of the importance of this training and also the running of a training course with increased capacity for a specific section.

Feedback from staff attending courses is gathered for each training course held. Feedback gathered has generally been positive and this is demonstrated by some analysis below:-

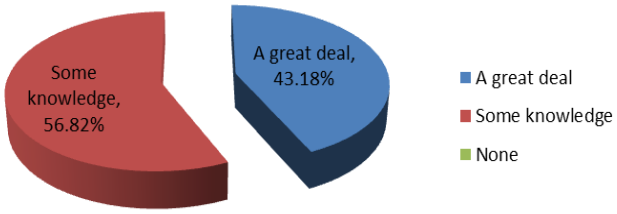
How well did the trainers know their subject?



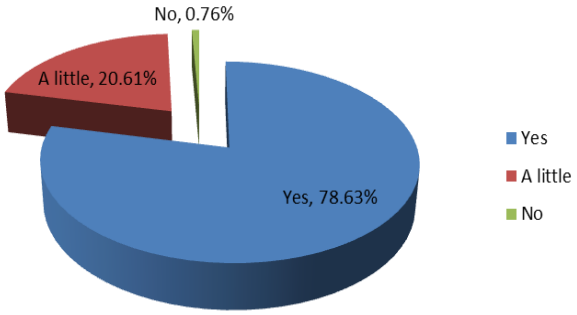
How well did the trainers convey their knowledge?



Do you think you have learned anything as a result of this course?



Will you be able to apply any new knowledge gained in your workplace?



Councillor Courses

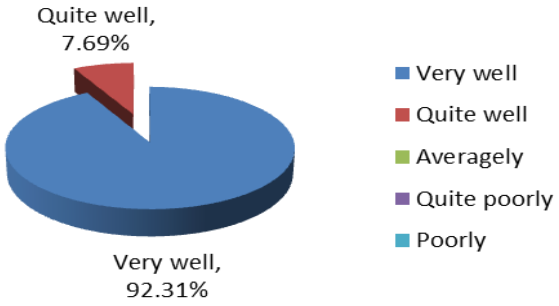
Councillor courses took place in 2013/14 and were well received. This year no courses were run and consequently plans are in place for councillor training in 2015/16.

Schools Courses

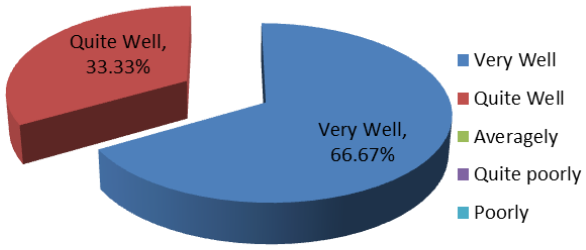
The first specific information security courses were run in June 2014. This shows a commitment on behalf of the council to supporting its schools meet their information governance requirements. The courses covered data protection, information security and meeting the needs of information legislation such as the Freedom of Information Act. 63 members of staff in total attended the training sessions which were supported by the Education Service and the Schools IT Team.

Feedback from staff attending courses is gathered for each training course held. Feedback gathered has generally been positive and this is demonstrated by some analysis below:-

How well did the trainers know their subject?



How well did the trainers convey their knowledge?



Do you think you learned anything as a result of this course?

Ad Hoc Courses and Presentations

As well as regular standard training sessions ad hoc sessions are provided for specific groups of staff and can be for anything from 2 – 100 people at once. These tend to be slightly less detailed and designed to highlight key messages.

One ad hoc course was run for staff within the GEMSS service and this was attended by 53 staff. This compares with 14 staff who attended an ad hoc course in 2013/14 and 180 staff who attended in 2012/13.

By their nature these courses vary in demand and staff have been encouraged to attend the corporate courses where possible. These are more detailed and are run regularly. As detailed above, the number of staff attending the standard corporate course has increased over the last three years.

The training provision is complemented by regular updates on the ‘My Information’ intranet pages which include support and guidance on all aspects of Information Management. Details of the guidance provided to staff are maintained to provide evidence of key messages provided to staff.

E-Learning

All staff who need access to the council's computer network are required to undertake e-learning before they can access the council network. This gives staff an appreciation of their obligations in conjunction with a signed form to request access and agree to abide by the council's guidance. Whilst the preference is to provide classroom training, it is recognised that e-learning can be complementary. A requirement remains to review e-learning content in 2015/16.

Information Policy Development

Policies form an invaluable way of documenting legal requirements and best practice. They provide guidance for employees to ensure information governance is integrated into the way the council operates. As well as developing new policies, it is also necessary that existing policies are updated to ensure remain fit for purpose.

Records Management Policy

A new records management policy was created this year to ensure that the council manages it records properly. This includes paper and electronic records. Benefits of the policy are as follows:-

- Effective records management provides evidence of what the council does and why
- Protecting the interests of the council and its staff as well as those who interact with the organisation.

The key messages of the policy are:-

- A record is information created, received and maintained as evidence
- Records can be in paper or electronic format
- Records kept must be accurate, authentic, reliable, complete, unaltered and usable
- All staff have a part to play in the management of records
- The Modern Records facility is administered by Document Services
- Information retention and disposal is a key part of records management as detailed in the information retention and disposal policy.
- For further guidance contact the information management team.

Records management is also being considered by the ICO and Public Services Ombudsman as key to good administration and further guidance is expected in 2015.

Updated policies

A major review of the Security Incident Reporting Policy was carried out to simplify the process and make roles and responsibilities clearer.

Policies are also reviewed to ensure that they are still valid and up to date. The following policies have been reviewed and amended over the last year:

> Access to Network, Information Risk Management (links to corporate risk management), Mobile Technology Policy (links to agile working), Remote Access, IT Physical Access, Password Policy (following WAO feedback), Email

All policies use 'key messages' for ease of understanding and are published as part of the overarching Information and IT Security Policy and on the Council's intranet, with appropriate version control. Policies and guidance to be developed and reviewed include Protective Marking and confidential waste.

2.4. Information Risk Register

Last year's report and the newly developed information risk management policy identified the need to develop an information risk register. This has been developed during this year and has been updated accordingly. This identifies key information risks, their likelihood, impact and the measures in place to mitigate the risk. This has been maintained and risks have been escalated at times including the period of the NATO summit held in Newport. The risk register is shared with the Information Governance Group so they are aware of the current status of risks and is maintained by the Information Management team.

Information risks are now included in the council's Annual Governance Statement and the Corporate Risk Register which demonstrates an increasing joining up of risks and an appreciation of their relationships. This is also assisted by the Chief Internal Auditor being a member of the Information Governance Group. High level information risks may be escalated up in to the Corporate Risk Register. In the May 2015 update of the corporate risk register, information risk was considered a medium risk (probability medium (3) and impact low (2)). The control strategies for information risk are noted in the corporate risk register as:

- Information Risk Management Policy
- Annual Information Risk Report and associated action plan
- Senior Information Risk Owner role (SIRO)
- Information Governance Group
- Staff training and awareness raising
- Policies and Procedures

2.5. Security Incidents

The Information Security Incident Reporting Policy establishes the requirement for all security incidents to be reported, logged and investigated. As detailed above this policy and associated forms have been updated over the last year and communicated to staff. Security incidents range from lost phones/other devices and password issues to data breaches where data is lost or passed to the incorrect recipient.

66 security incidents were recorded in 2014/15. This compares with 64 in 2013/14 and 63 in 2012/13. This shows consistency over the last three years. The 66 information security incidents are split in to the categories below as suggested by the ICO, with figures shown for 2013/14 for comparison:-

Category	**2014/15**	**2013/14**
Disclosed in error -	14	14
Lost or stolen hardware -	23	9
Lost or stolen paperwork -	0	6
Non secure disposal – paperwork -	2	1
Other - non principle 7 incident -	18	8
Other - principle 7 (security of personal information) incident -	0	4
Technical security failing -	9	22
TOTAL	**66**	**64**

Analysis by category is always to some extent subjective as incidents could easily be categorised in more than one category. Therefore these categories should be indicative only. There has been an increase in reported lost or stolen hardware and also an increase in non-principle 7 incidents which relate to human or process errors. There has been a reduction of incidents categorised as technical security failings.

The majority of security incidents recorded were not major concerns. Some of the themes are as follows:-

- Incidents arising as result of procedures not being followed correctly – human error
- E-mails sent to the incorrect recipient or including information that that shouldn't have been included
- Paper documents sent to the incorrect recipient or including information that that shouldn't have been included
- Lost mobile devices (with no personal data or blackberries so low risk)
- Lost remote access tokens which present a negligible security risk
- Some personal printed information left on printers internally
- Physical access issues with door entry system

No incidents were of significant concern to report to the Information Commissioners' Office (ICO). Two of the most significant incidents involved Social Services and reflects the amount and sensitivity of information being managed. One incident related to sensitive personal information that was verbally disclosed by a social care professional whilst in a difficult environment. Another related to information that included information in one document that was from another case. These again highlight the need for effective policies, procedures and staff training.

All information security incidents are investigated and follow up action including preventative measures are recorded. An overview is also reported to the SIRO and Information Governance Group. This work will also be reflected in the risk register and in communications with staff.

2.6. Information Sharing

The drive for more collaborative working across organisations requires that information is shared appropriately. The Wales Accord on the Sharing of Personal Information (WASPI) requires public sector organisations to follow agreed guidance in the development of Information Sharing Protocols (ISP's). The council signed up to WASPI in January 2011. The Information Management team leads on this work and has developed a number of ISP's with services and other organisations. This work is supported by the information sharing policy developed in 2013/14.

Finalised ISPs
Newport Drug & Alcohol Service
Multi Agency Risk Assessment Conference (MARAC)
Not in Education, Employment or Training (NEET)

Completed ISP's Awaiting Quality Assurance
None

Current and Future Developments
POVA
Provider Services
Team around the Cluster
Anti-Social behaviour, crime and disorder
Flying Start

2.7. Business Continuity

Due to the increasing reliance on information technology to support business activities, the council needs to ensure that activities can operate without access to their systems. In addition, the IT service needs to maximise the availability of the council's IT systems. A major piece of work has been carried out to analyse the council's critical services and identify the IT systems that support them.

Over the last year the draft priority IT systems was agreed by the Corporate Business Continuity Group and then by the council's Strategic Leadership Team. This is big step forward for the council as priority IT systems have not been documented and agreed previously. Importantly the priority systems are understood and used by the IT service operationally if issues with systems occur. The priority IT systems have also been circulated to services so they aware of the respective priority of their systems.

Work continues to review internal and external IT support arrangements to ensure that these are aligned to the priority of the IT systems identified. The development of IT monitoring tools has taken place and further work will take place in future to broaden the scope of this. Work has been carried out on systems with a higher than average perceived risk of failure and these will be completed in 15/16. Further work will also be carried out on infrastructure improvements and the testing of back-up and recovery of systems (WAO recommendation). Work has been carried out with Social Services to enable them to manage better if any of their critical IT systems are unavailable and further work will be carried out with them and other services in future.

Over the next year business continuity plans are being reviewed corporately. This will mean the need to review IT systems identified in the updated plans and make any changes necessary to agreed system priorities.

2.8. Technology Solutions

A number of technical solutions are in place to minimise risk to information and the corporate network generally as outlined below. PSN compliance and the development of business continuity requirements continue to drive technical improvements for information management. Wales Audit Office annually review the controls applied to key financial systems (reported to Audit Committee).

Mobility solution
The use of a mobility solution has been rolled out for agile workers that has improved the ability for users to access their information whilst away from their usual place of work. Staff are able to work from anywhere where a wireless network is available, as if they were sat at their desk.

Secure/Large File transfer solution
A new solution called Egress Switch has been procured to enable the secure transfer of e-mails and associated documents to organisations and individuals without secure e-mail facilities. This will place e-mails and documents on a secure web site for users to login in, access information and respond.

The solution provides the ability to restrict access to specific documents and audit access to the information provided. This was identified as a development item last year and this will provide a valuable facility for all staff. Initial roll out has commenced with full roll out planned during 2015/16.

Identity Management
Work has commenced on the roll out of Microsoft Forefront Identity Management (FIM) software. This will enable users to reset network passwords themselves and provide single sign on facilities in future.

Unified Communications
A Unified Communications telephony solution has been deployed to 1800 users across the council and provides enhanced communication facilities, including voicemail and unified communications.

Desktop technology
The council has increased the percentage of laptops as part of its total number of computers used. This is to encourage more flexible and agile working. Laptops now represent about one third of all desktop devices.

Laptops
- All laptops are protected using an end point protection solution
    - Includes encryption and anti-virus
    - Encryption solution is being migrated to Microsoft BitLocker
- Devices managed using Active Directory group policy management
- Mobile VPN for secure flexible and remote working as above

Desktop PC's
- All desktop PC's are protected using an end point protection solution
    - Includes anti-virus
    - Storage on networked home drives is recommended

Remote Access Solutions
The council's secure VPN (Virtual Private Network) solution is used by ad-hoc home workers and suppliers to identify and resolve issues with systems which they support. Supplier accounts are disabled when not in use and they need to ring IT before they are given access. All users needing access have to be authorised and are issued with a token for two-factor authentication, a small number of suppliers who may be required to support IT systems outside IT hours are also issued with a token.

Firewalls
Corporate firewall appliances are in place to protect the council's network from untrusted networks and a separate firewall protects the PSN network.

Wireless Staff Access
Wireless Access points are provided in many council buildings. This includes appropriate security controls in place.

Wireless Public Access
Wireless public access is provided in select council locations and this is protected using appropriate security measures where users can create logins for a limited period.

Physical Security
Major buildings (Civic Centre and Information Station) are limited to staff with physical access tokens and alarmed outside of opening hours. As detailed in the physical access policy:

- IT facilities must be located in secure areas protected from unauthorised access
- Any visitors to IT and Information Management secure areas must be signed in and accompanied at all times
- Computer rooms are subject to additional security measures to protect them from unauthorised access, damage and interference.

The policy and Building Access policy also require staff to display identity badges at all times. As detailed above, improvements to security for security doors at the Civic Centre was implemented this year.

Technology Developments
The Information and IT strategies are currently under redevelopment as part of the Council's Digital Strategy, but the next phase of development is likely to include a move to more 'cloud' based technologies. There are inherent risks in this change, with other organisations effectively holding the council's data and part of the development work for 15/16 will be ensuring that the appropriate controls are in place.

Financial Systems
Wales Audit Office annually review the controls applied to key financial systems (reported to Audit Committee)

2.9. Records Management

Records management continues to develop with new records management policy guidance, and the on-going implementation of Electronic Document Management (EDMS) in services from Housing Benefits, Council Tax, Planning, Social Services and Education. The development supports the principle of effective use of information and information governance, including access controls and retention policies.

Work commenced in early 2013 to create a Modern Records facility in the former rates hall at the Civic Centre. The room has been equipped with racking for the storage of archive paper records. This has been complemented by the acquisition of an IT application to record the location and content of files. This system enables fast retrieval of paper archive documents.

By April 2015 about 40% of the archive documents have been migrated to specific locations in the new facility, box contents recorded on to the Modern Records IT system. The remainder of paper archive documents are in temporary storage within the Civic Centre. The migration of these documents will continue through 2015/16.

2.10. Freedom of Information and Subject Access Requests

There are risks associated with responding to Freedom of Information and Subject Access requests. With freedom of information requests, care should be taken not to include any personal information as part of responses for instance when sending out spread sheets that might originally include personal data. No issues have been recorded this year but staff are reminded of the care required when responding to requests.

The number of freedom of information requests received by the Council increased last year and continues the trend of year on year increases in the number of requests. The performance indicator target for 2014/15 was met again although the increasing number means this remains a challenge.

Work has taken place to signpost important transparency information on the council's web site including all council spend over £500. This work will continue with the view to making more data available to meet the "open data" initiative.

Subject Access Requests are requests for personal information requested by the data subject and care needs to be given to ensure that personal information relating to other data subjects is removed. The only information that should be shared is that specific to the data subject. A new personal information request form was developed and this assists with gathering suitable information to confirm identity and other information when requests are received. Work has been carried out to review Subject Access Request processes and this will be developed further in 2015/16.

3. Risk Management and Associated Action Plan

As detailed in the sections above, a large amount of important work was carried out during 2014/15 building on the work of previous years. The risks remain broadly as previously but the impact of reduced financial resources suggests that the likelihood of information security issues will increase. Information sharing also provides continued challenges due to increasingly complex working relationships between organisations. Changes to the PSN compliance regime mean very similar requirements as previously but with an increased onus on the council to manage its attitude to risk.

The commitment to information governance remains with on-going training, awareness-raising, policy development, management of security incidents, IT business continuity management etc. Actions identified in this report will be detailed further in the Information Management team's business plan.

3.1. Risk Management

Risk	Impact of Risk if it occurs* (H/M/L)	Probability of risk occurring (H/M/L)	What is the Council doing or what has it done to avoid the risk or reduce its effect	Who is responsible for dealing with the risk?
Staff unaware of information risks and data breach occurs	H	L	• Provision of information security training • Staff awareness raising • Continue with specific information security training for Social Services • Development of new policies and update of existing ones • Additional Information security training and guidance for schools • Further improvements to processes for subject access requests	Information Governance Manager (IGM) in conjunction with Information Management team
PSN (Public Services Network) accreditation not gained	H	L	• Develop and document the council's approach to information risks • Evidence information governance arrangements as detailed in this document • Development of Information Governance Group to	Information Governance Manager (IGM) in conjunction with IT

			manage information risks • Members engaged to support these requirements	
PCI- DSS (Payment Card Industry Data Security Standards) compliance not achieved	M	M	• Submission of self-assessment questionnaire and successful compliance achieved • Continue technical scanning service to ensure no technical concerns	IGM in conjunction with Information Management team
Technical Solutions are not available to meet the needs of service delivery and data breach occurs	H	L	• Implement solution for file transfer • Encrypted laptop devices • Data stored on servers and not on local devices unless encrypted • Review solutions, identify and plug any gaps • Maintain health check and compliance requirements • Review the security of cloud based technical solutions considered	IT Infrastructure Manager in conjunction with Information Governance Manager
Information is not shared appropriately and securely	H	L	• Development of new information sharing protocols and review of existing ones • Advice and guidance	IGM in conjunction with Information Management team
Critical IT systems are not available to services	H	L	• Review and refine priorities for critical IT systems • Continue with action plan to improve availability of IT systems • Continue with services to develop business continuity arrangements	IT Infrastructure Manager in conjunction with Information Governance Manager and services
Information security is not considered for new projects	M	L	• Development and implementation of privacy impact assessments	Information Governance Manager in conjunction with services

3.2 Action Plan

Action	Deadline
Staff and councillor awareness	
Regular information security training sessions including revised content as necessary	On-going
Provide information security training courses for councillors as provided last year to widen understanding	tba with Democratic Services
Further policies and guidance will be developed to support the organisation including Protective Marking carried over from last year.	On-going
Existing policies and guidance will be reviewed and updated including reference to the information risk register to identify gaps in identified risk and supporting policies.	On-going
Investigation of security incidents and identification of issues to be followed up	On-going
Address improvements suggested by Wales Audit Office reviews	On-going
Continue to obtain employee feedback on information security issues, and use to inform risk management. Re-run information security awareness survey	Mar 16
Social Services information security training	On-going
Follow up information security training sessions for schools	Dec 15
Review e-learning provision	Mar 16
Standard policies and guidance for schools	Dec 15
Refine processes and improve management of Subject Access Requests	Dec 15
PSN accreditation and improved information governance	
Follow up on actions identified for PSN accreditation	Jun 15
Quarterly meetings of the Information Governance Group to oversee information risk management in conjunction with other stakeholders	On-going
Follow up actions as a result of the Wales Audit Office review	Sep 15
Review the Chair role of the Information Governance Group as suggested by the Wales Audit Office	Aug 2015
Management of the information risk register	On-going
Information asset owners to be defined for critical IT systems	Dec 15
Review requirements for PSN compliance review 2016, to include BYOD for members/staff as required	Jan 15
Members updated through Annual Information Risk Management Report, including review by Scrutiny Committee.	On-going
SIRO and Deputy Leader to be briefed on relevant information governance issues	On-going
PCI accreditation	
Pursue version 3 of Payment Card Industry Data Security Standard	June 15
Technical Solutions	
Roll out of Egress solution across the council	Mar 2016
Roll out of Microsoft FIM identity management solution	Mar 2016
Consider options and controls required for cloud-based systems where appropriate	On-going
Review technical solutions to ensure they meet information governance needs	On-going
Consider the need for new technical solutions to address weaknesses	On-going

Information Sharing	
Further Information Sharing Protocols will be developed to support collaborative working	On-going
Review existing Information Sharing Protocols	On-going
Business Continuity	
Refine and update Priority IT systems	Dec 15
Continue the action plan identified in the IT systems business continuity report	Dec 15
Test business continuity plans (Wales Audit Office recommendation)	Mar 16
New projects	
Privacy Impact Assessments to be carried out for new projects with template to be developed (note item carried forward from last year)	Dec 15