Report

Cabinet Member for Community & Resources

Part 1

Date: 28 November 2017

Subject **Annual Information Risk Report 2016-17**

Purpose To provide an assessment of the Council's information governance arrangements, identify key risks and agree the action plan for 17/18

Author Information Development Manager

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; use, retention, archiving and deletion.

The purpose of the council's fifth 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 **To endorse the Annual Information Risk Report 2016-17 and proposed actions.**

Action by Information Development Manager
Head of People and Business Change

Timetable As reported

This report was prepared after consultation with:

- Head of Law and Regulation – Monitoring Officer, and Senior Information Risk Owner (SIRO)
- Head of Finance – Chief Financial Officer
- Head of People and Business Change
- Chief Internal Auditor
- Information Governance Group
- Scrutiny Committee Planning and Development

Signed

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 the 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;
- Enable comparison of performance over time;
- Identify and address weaknesses and develop an annual 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 risk is not managed effectively.

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.	Digital and Information Manager and Information 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	Digital strategy sets the overall direction for the management of information. Day to day operational guidance provided by Digital and Information service.	Digital and Information Manager and Information team

* Taking account of proposed mitigation measures

Information Risk is also incorporated into Corporate Risk Register reporting, 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 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 actions outlined in this report form part of the People and Business Change service plan from 17/18.

Options Available and considered

1. **Do nothing**
2. **Note the annual information risk report and endorse its findings.**

Preferred Option and Why

The preferred option is option 2 – note the Annual Information Risk Report 2016/17 and endorse its findings. 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, FOIA, PSN accreditation and information sharing protocols. No further significant security breaches were referred to the ICO within the 12 month period covered by this Annual Report, although there are on-going actions being taken to resolve the issues previously identified. The updated action plan also sets out the on-going measures being taken to maintain and improve the integrity of the Council's information security systems and to deliver further training to increase awareness and compliance.

Comments of Head of People and Business Change

There are no direct staffing implications as a result of this report. The Annual Information Risk Report is a key element of the Council's risk management and demonstrates a sound approach to the management of information risk.

It is recognised that the Council's risk management approach at an organisational level needs to develop the five ways of working of the Well-being of Future Generations Act, however the approach taken does incorporate elements of the Act as outlined below.

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.

Comments of Cabinet Member

I support the need for robust processes to ensure that information is managed appropriately throughout the organisation. This includes moving to digital solutions and the removal of paper wherever possible. A

vital component is to ensure that all those handling information are aware of their own responsibility and that of their service. This is an important role of the Information Governance Group and the Information Governance team.

Local issues

No specific local issues.

NB***: Do not circulate for ward member comments until the report is drafted in accordance with the wishes of your Head of Service or Corporate Director and with the knowledge of the relevant cabinet member.***

Scrutiny Committees

The draft report was considered by the Scrutiny Committee for Community Planning and Development in June 2017 who endorsed the report and proposed action plan.

The questions and comments of the Scrutiny Committee were as follows:

- 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. **Update as requested: The latest figures show 75% of Social Services staff in scope have been trained to date.**
- 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 E-gress 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.

Equalities Impact Assessment and the Equalities Act 2010

The Equality Act 2010 contains a Public Sector Equality Duty which came into force on 06 April 2011. The Act identifies a number of 'protected characteristics', namely age; disability; gender reassignment; pregnancy and maternity; race; religion or belief; sex; sexual orientation; marriage and civil partnership. The new single duty aims to integrate consideration of equality and good relations into the regular business of public authorities. Compliance with the duty is a legal obligation and is intended to result in better informed decision-making and policy development and services that are more effective for users. In exercising its functions, the Council must have due regard to the need to: eliminate unlawful discrimination, harassment, victimisation and other conduct that is prohibited by the Act; advance equality of opportunity between persons who share a protected characteristic and those who do not; and foster good relations between persons who share a protected characteristic and those who do not. The Act is not overly prescriptive about the approach a public authority should take to ensure due regard, although it does set out that due regard to advancing equality involves: removing or minimising disadvantages suffered by people due to their protected characteristics; taking steps to meet the needs of people from protected groups where these differ from the need of other people; and encouraging people from protected groups to participate in public life or in other activities where their participation is disproportionately low.

Children and Families (Wales) Measure

No specific consultation with children and young people is relevant as part of this report.

Wellbeing of Future Generations (Wales) Act 2015

The current information risk management framework has not specifically incorporated the five ways of working as a core approach. However, the report highlights:-

- Long term – organisationally this is a long term development with increased maturity of information risk management
- Prevention – preventative measures are key to information risk management especially around staff awareness
- Integration – managing information risk is part of the council's wider risk management process
- Collaboration – information risk is managed in conjunction with the council's IT service delivery partner, the Shared Resource Service (SRS) as well as with suppliers who process data on behalf of the council
- Involvement – the council has direct contact with members of the public and businesses in relation to handling information although this is somewhat reactive

Crime and Disorder Act 1998

No specific considerations.

Consultation

Comments from members of the council's Information Governance Group have been included within the text of the report in line with their role as key strategic stakeholders.

Background Papers

Information Risk Management Policy (reviewed November 2015).
Annual Information Risk Report 15/16
Annual Governance Statement 16/17
Corporate Risk Management Strategy and Register
Digital Strategy 2015-2020

Dated: 28 November 2017

Annual Information Risk Report 2016/17

Created by	Information Governance
Date	03/04/2017
Reviewed by	
Date	

Document Control

Version	Date	Author	Notes / changes
V0.1	03/04/17	Mark Bleazard	Initial draft based on previous report
V0.2	11/05/2017	Mark Bleazard	Further updates
V0.3	19/05/2017	Mark Bleazard	Draft prepared for Information Governance Group
V0.4	30/06/2017	Mark Bleazard	Information Governance Group feedback and updates for Scrutiny
V0.5	04/07/2017	Mark Bleazard	Further updates for Scrutiny & Cabinet Member
V0.6	04/10/2017`	Mark Bleazard	Report comments for review and sign off by Cabinet Member
V0.7	02/10/2017	Mark Bleazard	Monitoring Officer Comments added for final sign off by Cabinet Member

Table of Contents

Executive Summary

The council has a statutory requirement to look after the data it holds in line with the Data Protection Act. **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. From May 2018, EU General Data Protection Regulation enables much higher fines of 20 Million Euros or 4% of turnover.**

This is the fifth Annual Information Risk Report which provides an assessment of the information governance arrangements for the Council as outlined in the Information Risk Management Policy. This provides an opportunity to identify changes made over the last five years and progress made during this period. **Please Note**: these sections are entitled '**5 Year summary'** and are formatted in shaded text as here. The report highlights:

- Accreditation and audit
    - Public Services Network (PSN) accreditation achieved. A number of vulnerabilities to resolve
    - EU General Data Protection Regulation will require a significant amount of work to comply with it
    - Payment Card Industry (PCI) data security standard lapsed and action plan to be completed following independent audit
    - Wales Audit Office – progress on disaster recovery/business continuity with implementation of technical solution to provide greater resilience
    - **5 year summary** – PSN compliance maintained, creation and management of Information Governance Group
- Information Governance culture and organisation
    - Became a partner of Shared Resource Service (SRS) which results in need to develop and maintain a key strategic and operational relationship with SRS
    - Information Asset Owners identified and Information Asset Register created.
    - **5 year summary** - creation of the Information Asset Register
- Communications and Awareness Raising
    - Continue to raise awareness with staff and Members
    - Large amount of training provided to staff
    - Training for Members provided
    - Review of policies carried out including Protective Marking Policy
    - E-learning reviewed and re-published
    - **5 year summary** – 699 staff have attended corporate training courses, 534 in Social Services, 32 councillors and 135 in schools. 6 new policies developed and existing policies updated
- Information Risk Register
    - Continues to be maintained
    - Contribution to Annual Governance Statement
    - **5 year summary** – information risk register created and managed
- Security incidents
    - Lowest number of recorded incidents this year
    - On-going management of incidents
    - One serious incident reported to the Information Commissioner's Office (ICO) last year closed by ICO with no formal action taken against the council

    - **5 year summary** – 298 incidents recorded over the last 5 years. 2 most serious incidents referred to the ICO with no action taken against the council.
- Information Sharing
    - Development of Information Sharing Protocols (ISP's) continues along with Data Disclosure Agreements (DDA's)
    - **5 year summary** - 12 ISP's developed and 9 DDA's
- Business Continuity
    - As a result of previous guidance from the Wales Audit Office, the council has commenced a large project to improve business continuity
    - **5 year summary** - the council's priority IT systems were formally identified for the first time
- Technology Solutions
    - Egress rolled out to all users as planned and training provided to 98 staff. Extended use of Egress solution for Data Loss Prevention scheduled.
    - Roll out of Xerox Mail solution in Revenues, Benefits and other areas. Extend roll out of solution to improve mail distribution further and reduce errors from manual paper handling
    - Consider options and controls required for cloud
    - Consider options for collaboration and simplification as a result of partnership with Shared Resource Service
    - **5 Year Summary** – increased the percentage of laptops used. Wireless facilities have been provided in council and other buildings as part of Newport Community Cloud. Egress Switch solution rolled out to all users.The Xerox Mail solution being rolled out.
- Records Management
    - Continued roll out of Electronic Document Management Solutions (EDMS) solution across council
    - Some capacity issues for Modern Records facility being addressed
    - **5 year summary** – Roll out of EDMS in 7 areas of the council. Development and management of Modern Records facility
- Freedom of Information
    - Missed target for first time in 5 years. Double the number of requests from six years ago.
    - Publication of open data sets where appropriate
    - **5 year summary** – met FOI target in 4 out of 5 years. 7 new data sets published
- Subject Access Requests
    - Improved processes implemented in Social Services with further roll out required
- New Projects
    - Privacy Impact Assessment completed for public Wi-Fi across the city

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 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.

The actions outlined in this report form part of the People and Business Change service plan and 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.

1.1. Purpose of the Report and Benefits

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
- This is the fifth Annual Information Risk Report which provides an opportunity to identify changes made over the last five years and progress made during this period. **Please Note**: these sections are entitled '**5 Year summary'** and are formatted in shaded text as here.
- 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. Currently the Information Commissioners Office (ICO) can issue a fine of up to £500,000 for data breaches. The fines associated with General Data Protection Regulation (GDPR) come in to place in May 2018. The maximum fine is 20 Million Euros or 4% of turnover. In cases where data breaches are referred to the ICO, its investigations highlight the importance of effective governance arrangements to reduce risks
- Ensure that appropriate risks are escalated to the Corporate Risk Register

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. In 2015 the Digital Strategy was developed which highlights the importance of effective information management and data sharing with robust information security to protect business and citizen data from threats, loss or misuse.

2.1. Compliance and Audit

The council is subject to accreditation to the Public Services Network (PSN) by the Cabinet Office. The council is also required to comply with the Payment Card Industry Data Security Standards (PCI-DSS) 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

Successful accreditation for PSN was received on 6th May 2017 and therefore the council's PSN compliance expires on 6th May 2018. Accreditation will be followed up by checks of the council's Remediation Action Plan to ensure continued compliance. The Remediation Action Plan identifies vulnerabilities in the council's systems with a timetable and tasks to resolve these vulnerabilities. There are always challenges to compliance given the variety of risks and work is required throughout the year to protect the council's data and systems. Continued compliance demonstrates a clear commitment to information security by the council.

European Union General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is a regulation by which the European Parliament, the European Council and the European Commission intend to strengthen and unify data protection for individuals within the European Union (EU). The GDPR will apply in the UK from 25 May 2018. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

There are major implications as a result of GDPR and this will be a standard agenda item for the Information Governance Group.

A summary of some of the changes are detailed below:

- The maximum fine is 20 Million Euros or 4% of turnover.
- Greater requirement to document the personal data held
- Data breach reporting will become mandatory for certain data breaches
- Enhanced rights for data subjects including improved privacy notices and increased focus on consent that must be unambiguous and not assumed
- Specific guidance relating to children and their rights
- Requirement to establish legal basis for sharing beyond "legitimate interests"
- The removal of maximum fee for Subject Access Requests and reduction in days to process (from 40 calendar days down to 30)
- Requirement for Data Protection Impact Assessments
- Requirement for Data Protection Officer
- Further consideration of data stored outside the EU

Payment Card Industry Data Security Standards (PCI-DSS)

The council has been compliant with Payment Security Industry (PCI) Data Security Standards since December 2014. As detailed in last year's report, the council, in conjunction with its internal audit team, commissioned an external audit of its PCI compliance. This was designed to ensure strict adherence to the standards and any areas requiring improvement. Following this audit, issues were identified that needed addressing. An action plan was developed for these issues and was reviewed by the council's Information Governance Group and this is planned to be completed by July 2017. Due to these issues, the council's PCI compliance has lapsed to ensure these issues are formally resolved to meet PCI requirements. Security scans continue to be carried out quarterly to ensure card data is secure when it is transmitted across the internet to the council's payment providers. No issues have been addressed by these scans which mitigates the risk of current non-compliance.

Wales Audit Office (WAO)

The Wales Audit Office (WAO) carries out audits annually which involve IT and Information Governance. The WAO visited to review a number of items in May 2016. One key area of improvement expected is to the council's business continuity and disaster recovery plans. A project commenced to provide improved arrangements and this is being implemented as part of the council's new partnership with the Shared Resource Service (SRS) detailed in the 'Organisation' section below. Details of the improvements being made are detailed further in the Business Continuity section of this report.

2.2. Information Governance Culture and Organisation

5 Year Summary - The council's information governance arrangements continue to mature. This, the fifth annual information risk report, provides an opportunity to reflect on changes made over the last 5 years. During this period the Senior Information Risk Owner and Chair of the Information Governance Group have been separated from the operational management of the Information Governance team to provide independence. An Information Governance Group has been formed and now meets regularly. Staff have been surveyed for their views of information governance in the organisation. An Information Asset Register was created during 2016/17. These changes demonstrate a number of improvements made over the last 5 years.

A major change will result from the council entering in to a partnership with the Shared Resource Service (SRS) as detailed further below. The client side role sits within the Digital and Information team and this relationship will be developed to ensure the best use of digital technology to support the council.

Information Governance Culture

The information governance culture has previously been investigated by virtue of staff surveys. These demonstrate good staff awareness of information governance issues and good buy in.

5 Year Summary – two staff surveys have been carried out with results of the second survey identifying improvements over the previous survey.

Organisation

The council's Senior Information Risk Owner (SIRO) role, responsible for Data Protection within the organisation, is part of the Head of Law and Regulation role. Day to day operational management is provided by the Information Governance team that reports to the Head of People and Business Change.

Shared Resource Service - As highlighted in last year's report the preferred option for the delivery of its IT Service was to become a partner in the Shared Resource Service (SRS) which is currently made up of Torfaen County Borough Council, Monmouthshire County Council, Blaenau Gwent County Borough Council and Gwent Police. This change was agreed by the council and the council's IT service migrated to the Shared Resource Service formally on 1/4/2017. This represents a significant organisational change in the delivery of IT services. New representation on the council's Information Governance Group will be established with the SRS and information will be shared between partners to provide further improvements to information governance. The client side role is managed by the Digital and Information team and this important relationship in service delivery as well as information governance will develop over time.

Information Asset Register - the development of an Information Asset Register, based on a template from The National Archives has now been completed for priority systems. This is a further improvement to the council's information governance arrangements. This identifies the owner of information, the information stored within the system, how this is shared and various other pieces of information. This will be extended and enhanced in future. This is required in preparation for the General Data Protection Regulation (GDPR) which is new EU data protection legislation mentioned above.

An important aim of this report is to ensure that members and senior officers are aware of the information security responsibilities of the council and to enable guidance to be provided. This is especially important this year due to the council elections in May 2017 and changes to members. 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. This has been beneficial in shaping the actions going forward.

The Information Governance Group has met quarterly since its inception in November 2013. The chair of the Information Governance Group is the Strategic Director – Place. This is to ensure there is no possibility of a conflict of interests of the operational lead for information governance also being the chair of this group. Strategic information governance issues are discussed by this group with standard agenda items being compliance update, information security incidents, training and awareness raising, risk report monitoring and other information governance updates. Membership of the group has been reviewed to ensure there is appropriate representation from the Shared Resource Service (SRS) which will be a major contributor to this work.

Schools are "data controllers" under the Data Protection Act and therefore need to be equipped to handle data appropriately. To support schools, guidance is provided by staff in Education and Information Governance.

2.3. Communications and Awareness Raising

As demonstrated in the Information Security Incidents section later, employees can be the weakest link in terms of preventing incidents. Therefore, awareness for employees is vitally important as technical measures will never be totally effective. This can be improved by staff training and other forms of communication to improve awareness.

Staff Guidance

Regular reminders of good practice have been provided in the weekly staff bulletin and on the intranet on various important subjects. As noted last year, in response to the incident reported to the ICO, further guidance has been provided in terms of handling paperwork. Staff guidance was provided in relation to the risk of phishing e-mails following an incident with ransomware (as detailed in the incidents section later). Some printing incidents have also been highlighted.

An information security leaflet is provided to all staff attending training and is provided to 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 including good and bad practice.

Training Courses

The council continues to provide classroom style training to staff to provide the most interaction possible and improved learning experience. This complements e-learning required to be completed by new starters. The content has also been reviewed and updated to reflect recent events and make it as relevant as possible. The courses run are:-

- Social Services courses
- Corporate courses
- Councillor courses
- Schools courses
- Ad hoc courses and presentations
- Egress training
- Information Governance team training
- Use of Electronic Document Management
- E-learning

Training courses represent a continued commitment to information security by the council. Training is a key area as people are generally considered the weakest link in relation to information security. There will never be totally comprehensive technical measures to protect data. Training provided to staff is a key part of investigations carried out by the Information Commissioner's Office (ICO) as highlighted in the 'Security Incidents' section below. Attendance on training courses this year is very similar to that for last year for both Social Services and corporate courses.

Social Services Courses

Social Services employees continue to represent a high risk group due to the nature of the information they handle as part of their roles. Therefore, training is compulsory for these staff. A serious incident reported to the Information Commissioner's Office (ICO) in 2015/16 required the council to pay particular attention to training of Social Services staff. As a result, prioritisation of staff training has been carried out and additional courses scheduled until the end of 2017 to meet these demands. In 2016/17 the number of staff attending was 144 compared with 147 in 2015/16.

5 Year Summary - Since specific training started for Social Services in April 2013 a total of 699 staff in Social Services have attended training. A breakdown per year is included below.

Year	Number of staff who attended
2016/17	144
2015/16	147
2014/15	182
2013/14	226
2012/13	0
Total	699

Feedback from staff attending courses is gathered for each training course held. Feedback gathered has generally been positive and this is demonstrated in Appendix B below:-

Corporate Courses

These courses are scheduled on a monthly basis, primarily for staff other than Social Services although the content of courses was consolidated in 2015/16. The number of staff attending the corporate course was 118 compared with 114 in 2015/16. Work has already commenced targeting senior managers in the council. Regular reminders and checks on attendance will continue to be carried out.

5 Year Summary - Since April 2012 the number of staff attending the corporate training course is 534. A breakdown per year is included below.

Year	Number of staff who attended
2016/17	118
2015/16	114
2014/15	152
2013/14	93
2012/13	57
Total	534

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 in Appendix A below:-

Councillor Courses

Councillor training took place in September 2016 and 14 councillors attended. Courses were also carried out in October 2013 attended by 18 councillors. All councillors, like all council staff, need to undertake mandatory e-learning before they are provided with access to the council's network.

5 Year Summary - Since April 2012 the number of councillors that have attended information security training is 32.

Schools Courses

No specific information security courses for schools were run during 2016/17. Courses were previously run in December/January 2015/16 and in June 2014

5 Year Summary - Since April 2012 the number of staff from schools that have attended information security training is 135.

Other Courses and Presentations

For consistency and operational purposes staff are encouraged to attend standard corporate course where possible. Where operational issues make this difficult and for broader coverage, ad hoc courses are sometimes run. During this year an hoc course was run for staff in the Registrars and this was attended by 21 staff.

5 Year Summary - Since April 2012 the number of staff attending ad hoc training course is 268. A breakdown per year is included below.

Year	Number of staff who attended
2016/17	21
2015/16	0
2014/15	53
2013/14	14
2012/13	180
Total	268

Egress Training
To support the increased use of the Egress Switch solution, training content was developed and training was provided to 98 members of staff. This has also been complemented by e-learning for Egress developed.

Information Governance Team Training
Two members of the Information Governance team successfully passed the British Computer Society (BCS) Certificate in Data Protection this year. **5 Year Summary** - following the success of the other team member last year, this means that the whole team are formally qualified in Data Protection.

Electronic Document Management System (EDMS) Training
During this year 39 people have been trained on the Electronic Document Management System. E-learning was developed for the roll out of EDMS in Payments.

E-Learning
All staff that need access to the council's computer network are required to undertake e-learning before they can access the 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. As detailed last year, the e-

learning required an update and this was carried out. Whilst the preference is to provide classroom training, it is recognised that e-learning can be complementary especially to get an initial appreciation.

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 that they remain fit for purpose, including any changes as a result of the partnership with the Shared Resource Service (SRS). Staff are reminded of these policies where appropriate.

Updated policies

As identified in last year's report, a major review of the council's Protective Marking policy was completed following changes to the government's protective marking scheme. Policies are also reviewed generally to ensure that they are still valid and up to date.

Staff are made aware of policy changes with reminders through the regular staff bulletin. 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.

5 Year Summary

Over the past 5 years the following policies have been created:-

- Information Retention and Disposal Policy
- Information Sharing Policy
- Confidential Waste Policy
- Information Risk Management Policy
- Records Management Policy
- Document Services – Physical Access Policy

2.4. Information Risk Register

An information risk register continues to be maintained that identifies key information risks, their likelihood, impact and the measures in place to mitigate the risk. The risk register is regularly shared with the Information Governance Group to keep them informed of risks and is maintained by the Information Governance team.

Information risks are considered as part of the council's Annual Governance Statement and the Corporate Risk Register. The Chief Internal Auditor is a member of the Information Governance Group which helps to join up services. High level information risks may be escalated up in to the Corporate Risk Register. Currently no information risks are identified as high level risks in the corporate reports. The control strategies for information risk are detailed within this report.

2.5. Information Security Incidents

All information security incidents need to be reported, logged and investigated. Information security incidents range from lost phones/other devices, password issues all the way to data breaches where data is lost or passed to the incorrect recipient. Lessons need to be learned from these incidents to improve practice in future to minimise the risk of recurrence.

43 security incidents were recorded in 2016/17 compared with 62 in the previous year. This is the lowest number of recorded incidents during the period that the information risk report has been produced. It is difficult to establish whether this reflects an improved position or a reduced level of reporting. Previous consistency over the number of incidents would suggest that the reduced number of incidents is a positive sign.

5 Year Summary - Details of reported incidents over the last 5 years are provided below:-

Year	Total incidents	Disclosed in Error	Lost or Stolen Hardware	Lost or Stolen Paperwork	Non secure disposal – paperwork	Other - non principle 7 incident	Other - principle 7 (security of personal information) incident	Technical security failing
2016/17	43	25	5	0	0	1	8	4
2015/16	62	23	12	2	0	9	11	5
2014/15	66	14	23	0	2	18	0	9
2013/14	64	14	9	6	1	8	4	22
2012/13	63	No split by category available						
Total	298							

As highlighted previously, 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 seen as indicative only.

The highest category continues to be incidents categorised as disclosed in error. These generally reflect human error in data handling. This further emphasises the need for training and awareness-raising for staff which the council continues to invest in. There is a further reduction in lost or stolen hardware which is good news.

As usual, the majority of security incidents were not of major significance. Some of the themes which are similar to previous years 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)
- Some personal printed information left on printers internally

The increased used of the corporate Electronic Document Management System (EDMS) and the use of the Xerox Mail solution will continue to reduce the amount of paper handled and reduce the potential for mail errors.

Probably the most significant incident during this year was a ransomware incident that occurred in August 2016. This incident caused significant disruption to services over a number of days. No data was lost as a result of this incident and no payment was made. Lessons learned were formally identified to minimise the risk of such an incident re-occurring in future.

There were issues with the council's door entry system for the Civic Centre but these were resolved after major improvements were made to the system.

No incidents were reported to the Information Commissioner's Office (ICO) this year. There was however a follow up on the incident reported to ICO last year when paperwork was stolen from a social worker's home as part of a burglary. Various actions were completed in relation to this incident. Staff who have not been trained previously have been identified and this training will be completed over the forthcoming year.

All information security incidents are investigated with incident reports compiled following discussion with those involved in the incident. An overview is also reported to the SIRO and Information Governance Group.

2.6. Information Sharing

Collaborative working is driving the sharing of increased amounts of information between the council and other organisations. 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 Governance team leads on this work and has developed a number of ISP's with services and other organisations. A full list of the Council's ISPs is published on the Intranet, the following represents developments in 2016/17:

Information Sharing Protocols (ISP's)

No Information Sharing Protocols have been completed and quality assured during this year.

Completed ISP's Awaiting Quality Assurance
Flying Start

5 Year Summary – the following ISP's have been developed and quality assured over the last 5 years:-

- Integrated Family Support Service (IFSS)
- Housing and Homelessness Action Group (HHAG)
- Provision of Housing (Common Housing register)
- Supporting Housing Gateway
- Not in Education, Employment or Training (NEET)
- Integrated Adult Learning Disability Service
- Single Point of Access and Community resource Teams (FRAILTY)
- Integrated Community Mental Health Service
- Integrated Occupational Therapy Service
- Tackling Substance Abuse
- Domestic Violence (MARAC)
- Education Achievement Service (EAS)

Data Disclosure Agreements (DDA's)

Data Disclosure Agreements (DDA's) are for one way disclosure of information from one organisation to another. These are recommended as part of the WASPI initiative and are seen as best practice for formalising such information disclosure.

Data Disclosure agreements have been developed as follows:-

Finalised DDA's in 2016/17:

Community Dentistry
WCCIS system
Policy in Practice
Supporting People Data Linkage Study with NHS Wales and Swansea University (SAIL Project)
Disclosure of Data between school and Assessment Foundation

5 Year Summary – the following DDA's have been developed over the past 5 years:-

Blue Badges
School Pupil Vaccinations
Careers Wales
Community First and schools
Community Dentistry
WCCIS system
Policy in Practice
Supporting People Data Linkage Study with NHS Wales and Swansea University (SAIL Project)
Disclosure of Data between school and Assessment Foundation

2.7. Business Continuity

There is an ever increasing reliance on digital technology to support business activities and this places increased reliance on the council's systems. It is therefore important to maximise the availability of systems. Increased resilience was a factor in the decision to become a partner of the Shared Resource Service (SRS).

As a result of previous guidance from the Wales Audit Office, the council has commenced a large project to improve business continuity. This includes improvements to existing infrastructure and new hardware. Improvements include the migration of backups from tape to disk for increased speed and accessibility and additional infrastructure which will provide access to systems should both server rooms at the Civic Centre not be available. This is a major change to infrastructure and will take place over a number of months. Priority systems will be reviewed with Service Areas and the Shared Resource Service. Priority system across partner organisations will be reviewed and agreed where possible.

As a result of a serious ransomware incident (detailed previously in this report), a formal review of the council's response was carried out in conjunction with the Civil Contingencies Unit. A report was produced to review the incident and identify lessons learned.

5 Year Summary – over the past 5 years the council's priority IT systems were formally identified for the first time. These systems have regularly been reviewed. A major improvement to the council's back up and recovery systems has been purchased for implementation.

2.8. Technology Solutions

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

Digital Champions
The council has commenced a programme of "Digital Champions" who are advocates for the use of digital technology. They provide a key contact point for services using digital technology. They will be one method of communicating messages to staff and also for testing the application of new systems.

Mobility solution
The use of a mobility solution has been rolled out for agile workers. This 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, which also reduces the requirement to carry paper documents.

Secure/Large File transfer solution
The roll out of the Egress Switch has now been completed with 2,230 users currently. This enables the secure transfer of e-mails and associated documents to organisations and individuals without secure e-mail facilities. The solution provides the ability to restrict access to specific documents and audit access to the information provided. It also allows large files to be safely shared via email. The solution has enhanced Data Loss Prevention (DLP) facilities to scan e-mail for personal data and enable its safe transfer. This solution will be rolled out in July 2017. In line with the implementation of Egress Switch generally, the council will remove personal network storage for staff wherever possible.

Identity Management
Microsoft Forefront Identity Management (FIM) software has been rolled out to enable users to reset network passwords themselves.

Xerox Mail "hybrid mail"
A new "hybrid mail" system was implemented during this year to streamline the production of paper and electronic outputs. This enables documents to be sent to production printers in the print room and then processed through the mail room folder/inserter machine. This improves security by ensuring that print outputs are split in to envelopes automatically in the folder/inserter machine. Roll out has taken longer than anticipated with roll out primarily in Revenues and Benefits. Other outputs are being migrated to this solution and this will continue over the next financial year. This solution provides financial savings and reduces information risk.

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 with access to information and records from a variety of locations. Laptops now represent about 65% of all desktop devices.

Laptops and desktop PCs

- All corporate laptops are protected using an end point protection solution
    - Encryption solution is used
    - A solution for schools laptops is under review
- Devices managed using Active Directory group policy management
- Mobile VPN for secure flexible and remote working as above
- All desktop PC's are protected using an end point protection solution
- Storage on networked home drives is recommended
- Unified Communications telephony solution has been deployed to 2200 desktop users across the council and including voicemail and the ability to access telephony from non council locations.
- 'Follow Me' print is available to all users, who are able to access Council printers from any location

Remote Access Solutions

The council's secure VPN (Virtual Private Network) solution is used by ad-hoc agile 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. Public Wi-Fi is also now available as part of the 'Digital Newport' work in the city centre (NewportCity Connect) 54 public buildings and on public transport (NewportCommunityCloud). Friendly Wi-Fi accreditation has been achieved for this set up.

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 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.

Digital and Technology Developments

The council's Digital Strategy outlines strategic objectives including a move to more 'cloud' based technologies. There are inherent risks in this change, with other organisations effectively holding the council's data. There will be on-going work to ensure that appropriate controls are in place.

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

5 Year Summary – over the past 5 years the council has increased the percentage of laptops used by the organisation as a total of all devices. Wireless facilities have been provided in council and other buildings as part of Newport Community Cloud. The Egress Switch solution has been rolled out to all users for secure e-mail facilities. The Xerox mail solution was procured and is being rolled out across the council. The Identity Management solution has been rolled out.

2.9. Records Management

Records management continues to develop with the ongoing implementation of the corporate Electronic Document Management System (EDMS) across an increasing number of services. EDMS provides the council with a modern, efficient, electronic system for managing documents, improving the way information and documents are used and the flow of information around the council. Documents are scanned on receipt into the mail room, and made available to services on the EDM system.

The Project Manager worked with services to identify their requirements and implement with the services accordingly. The biggest implementation for 2016/17 was in Payments for invoices. Also implemented was part of regeneration, Investment and Housing as well as reviewing and making changes to the implementation in Education.

For paper documents, work commenced in early 2013 to create a Modern Records facility at the Civic Centre. The room is 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 for retrieval of paper archive documents. By March 2017 over 5,500 boxes of archive documents have been migrated to the new facility. The rationalisation of accommodation and consolidation of paperwork has resulted in extra paperwork. This has caused capacity issues so an additional area to provide extra capacity has been identified. It is planned to set this up by the end of this year.

5 Year Summary – over the past 5 years the council has rolled out its Electronic Document Management System across a large number of services as below:-

- Building Control
- Education
- Transactional HR & Pay
- Licensing
- Planning
- Payments
- Part of Regeneration, Investment & Housing

The council has also developed a Modern Records Facility for paper archives.

2.10. Freedom of Information and Subject Access Requests

As a public authority, the Council also handles requests for information and data. 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.

Freedom of Information
This is the third time that the number of Freedom of Information (FOI) requests has been included. The number of requests received in 2016/17 was 1087 which shows a 19% increase since 2015/16. Performance for 2016/17 was 84.1% of requests responded to within 20 working days. This was below the target of 88% of requests.

This year's performance was as a result of an increasing number of requests received and specific issues in certain areas of the council. These are being addressed for improvement in 2017/18. An ever increasing number of requests continues to raise challenges for the organisation. During this year 211 of the requests were received via the online form.

5 Year Summary - Since April 2012 the number of Freedom of Information requests has risen significantly with a rise year on year. A breakdown per year is included below.

Year	Number of requests
2016/17	1087
2015/16	914
2014/15	895
2013/14	869
2012/13	698
Total	4463

In fact if we go back six years the number of requests received has doubled from 540 to 1087.

2016/17 is the only time the target has not been achieved in the past five years.

The Shared Resource Service is looking to provide a single Service Desk system for all partners. This may result in a new system for incidents and this may mean a new system is required for managing freedom of Information requests.

Publishing data
Government and ICO guidance encourage the publication of data as good practice for public bodies and this is referenced in the publication scheme as part of our commitment to openness and transparency. The transparency page www.newport.gov.uk/transparency was developed to improve signposting of council data.

This page now includes:-

- Council spend over £500
- Councillor allowances and expenses
- Business rates data
- Public health funerals

- Council pay and grading (new)
- Pupil numbers in Newport (new)
- Newport Matters production costs (new)

As detailed above new data has been made available this year and the intention is to add suitable data sets as they are identified. This data is free to re-use under the terms of the Open Government Licence.

Subject Access Requests
Subject Access Requests (SAR's) 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 General Data Protection Regulation means that there will be no fee chargeable from May 2018. The use of a personal information request form has worked well in identifying specific subject areas for requests as well as gathering details of the requestor. It is crucial to gather proof of identity so personal data is not disclosed to a third part accidentally. Social Services are using improved processes and systems for managing requests and it is planned to be rolled out to other areas.

3. Risk Management and Associated Action Plan

As highlighted above the organisation has carried out a comprehensive programme over 2016/17. The sections that provide a summary of progress over a five year period clearly demonstrate on-going commitment to information governance and continuous improvement. However, risks change regularly and it is important to monitor these and take appropriate steps to mitigate.

Compliance with standards continues to be a challenge given the tightening and refinement of these standards. A lot of work is required to maintain compliance with Public Services Network and Payment Card Industry standards. Wales Audit Office will continue to provide an independent review of practice.

The Information Commissioner's Office (ICO) formally closed the investigation in to the incident from 2015/16 which is clearly good news. This will be kept on file by the ICO and would be considered in the context of any future incidents serious enough to report to the ICO.

Many organisations including the council have a large amount of work to carry out to comply with the EU General Data Protection Regulation. This will require a considerable amount of work over the forthcoming year and will be challenging due to its wide-ranging requirements. The fines that can be imposed on organisations are significantly higher than those available to the ICO currently.

The Information Governance Group continues its important work of monitoring risk across services and providing strategic direction. The council's IT Service being provided as part of the Shared Resource Service (SRS) provides a new dynamic in information governance. The client side role needs to carry out an important strategic role as well as monitoring performance. The aim is for improvements in information security across all partners by a simplified and standardised infrastructure where possible.

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 Digital and Information 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 Further improvements to processes for subject access requests	Digital And Information Manager (DAIM) in conjunction with Information Governance team
PSN (Public Services Network) accreditation not gained	H	L	Progress resolution of vulnerabilities identified by IT health check taking special note of priority items Evidence information governance arrangements as detailed in this document Extension of Information Asset Register and improved governance arrangements Continued engagement with Members	Digital And Information Manager (DAIM) in conjunction with in conjunction with SRS
Delivery of IT Service by Shared Resource Service (SRS) provides less control	M	M	Develop relationship with the SRS Develop client side role to provide strategic input and performance monitoring	Digital and Information Manager (DAIM) in conjunction with Head of PBC / SRS management
Unprepared to implement EU General Data Protection Regulations	M	M	Review requirements further in conjunction with ICO guidance Develop detailed action plan to plug gaps Regular discussion at Information Governance Group	Digital and Information Manager (DAIM) in conjunction with Head of PBC / SRS management
PCI- DSS (Payment Card Industry Data Security Standards) compliance not achieved	M	M	Complete actions identified in audit report Resubmission of self-assessment questionnaire and successful compliance achieved Continue technical scanning service to ensure no technical concerns	Digital And Information Manager (DAIM) in conjunction with in conjunction with SRS
Technical Solutions are not available to meet the needs of	H	L	Roll out of Egress Data Loss Prevention (DLP) system for all users Continue roll out of Xerox Mail solution	Digital And Information Manager (DAIM) in conjunction

service delivery and data breach occurs			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	with Information Governance team
Information is not shared appropriately and securely	H	L	Development of new Information Sharing Protocols and Data Disclosure Agreements and review of existing ones Advice and guidance	Digital And Information Manager (DAIM) in conjunction with Information Governance team
Critical IT systems are not available to services	H	L	Continue to review and refine priorities for critical IT systems Implement disaster recovery/business continuity improvements at Shared Resource Service (SRS) Work with SRS to develop consistent IT system priorities across partners where possible	SRS in conjunction with Digital and Information Manager and services
Information security is not considered for new projects	M	L	Extend the implementation of privacy impact assessments Use ICO process including screening	Digital and Information Manager in conjunction with services

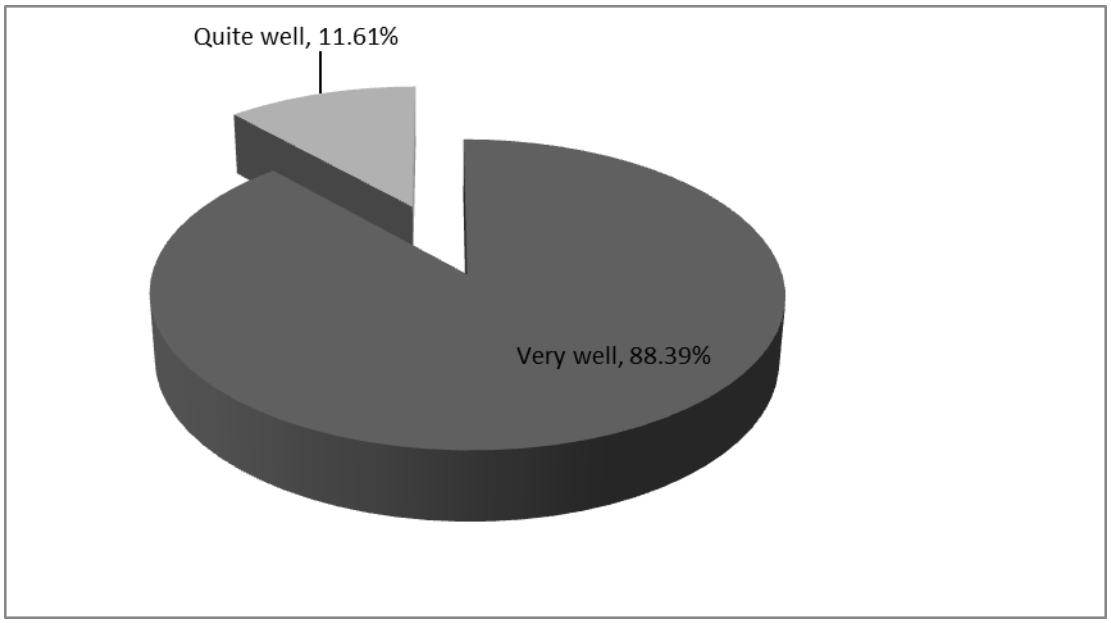
3.2 Action Plan

Action	Deadline
Compliance and Audit	
PSN accreditation	
Follow up on Remediation Action Plan to ensure continued PSN compliance	Jun 17
EU General Data Protection Regulation (GDPR)	
Review Information Commissioner's Officer guidance on GDPR	On-going
GDPR to be discussed as standard item at Information Governance Group	On-going
Information Asset Register to be extended	Mar 18
Document and review privacy notices across the organisation	Mar 18
Review the rights of individuals in line with GDPR	Mar 18
Remove the fee for Subject Access Requests prior to GDPR	Mar 18
Review legal basis for data processing	Mar 18
Review processes around consent	Mar 18
Review issues around children and consent	Mar 18
Comply with processes for mandatory data breach notification and revise information security incident reporting policy	Mar 18
Widen use of Privacy Impact Assessments now known as Data Protection Impact Assessments	Mar 18
Formalise position with Data Protection Officer role	Mar 18
PCI accreditation	
Payment Card Industry Data Security Standard resubmission following actions as a result of audit	Jul 17
Information Governance Culture and Organisation	
Develop and manage relationships with Shared Resource Service (SRS)	On-going
Contribute to information governance considerations across all SRS partners	On-going
Quarterly meetings of the Information Governance Group to oversee information risk management in conjunction with other stakeholders including Shared Resource Services representation	On-going
SIRO and Cabinet Member to be briefed on relevant information governance issues	On-going
Members updated through Annual Information Risk Management Report, including review by Scrutiny Committee.	Jul 17
Extension of Information Asset Register and Information Asset Owners in line with EU General Data Protection Regulation	Mar 18
Communications and Awareness Raising	
Regular information security training sessions corporately and for Social Services including additional monthly courses to meet demand	On-going
Target senior managers for information security training.	On-going
Provide regular reminders and checks on attendance corporately and in Social Services	On-going
Review need for information security training courses for councillors as provided last year	Jul 17
Further policies and guidance will be developed to support the organisation	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
Provide advice and guidance to support schools with the Education service.	On-going
Information Risk Register	
Management of the information risk register	On-going
Information Security Incidents	
Investigation of security incidents and identification of issues to be followed up	On-going

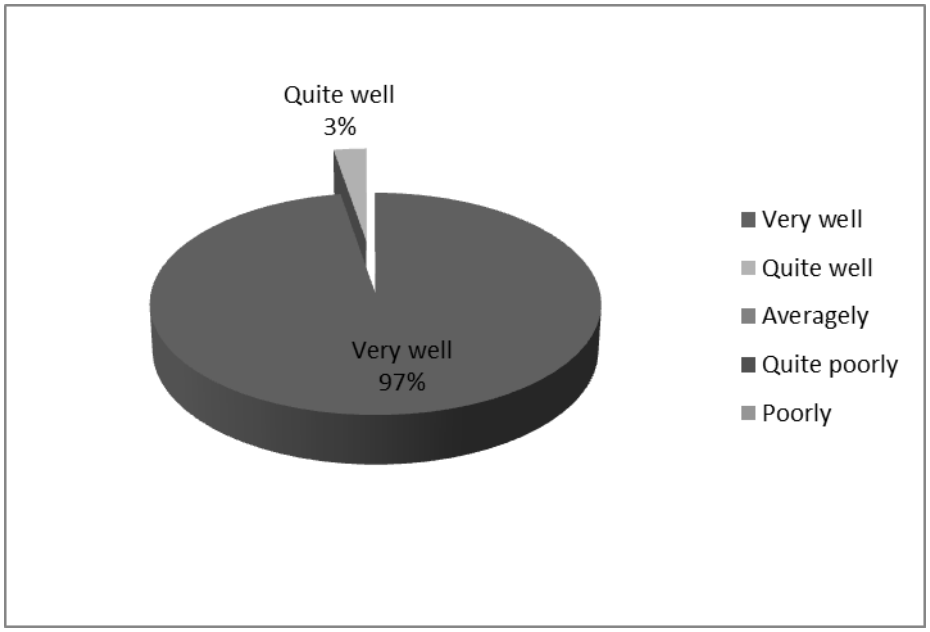
Information Sharing	
Further Information Sharing Protocols will be developed to support collaborative working	On-going
Review existing Information Sharing Protocols	On-going
Develop additional Data Disclosure Agreements as required	On-going
Business Continuity	
Make disaster recovery/business continuity improvements as a result of WAO.	Dec 17
Review priority systems with service areas and Shared Resource Service and agree priorities across partner organisations where possible	Dec 17
Technology Solutions	
Roll out of additional Egress Data Loss Prevention facilities	Jul 17
Reduce access to cloud based personal network storage systems for staff	On-going
Extend use of Xerox Mail solution to improve mail distribution processes	On-going
Consider options and controls required for cloud-based systems	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
Records Management	
Continued roll out of EDMS solution across council	On-going
Completion of extra capacity for Modern Records facility	Mar 18
Freedom of Information and Subject Access Requests	
Freedom Of Information	
Address performance issues in specific areas to improve overall council performance	Jul 17
Publication of further open data for suitable data sets	On-going
Identify and procure a new FOI system if required	Mar 18
Subject Access Requests	
Review Subject Access Request processes in line with GDPR	Mar 18
Extend use of EDMS solution for redaction of Subject Access Requests	Mar 18
Extend use of FOI request system for managing Subject Access Requests	Mar 18
New projects	
Carry out Data Protection Impact Assessment for relevant projects in conjunction with GDPR requirements	On-going

Appendix A - 2016/17 Corporate Training Evaluation

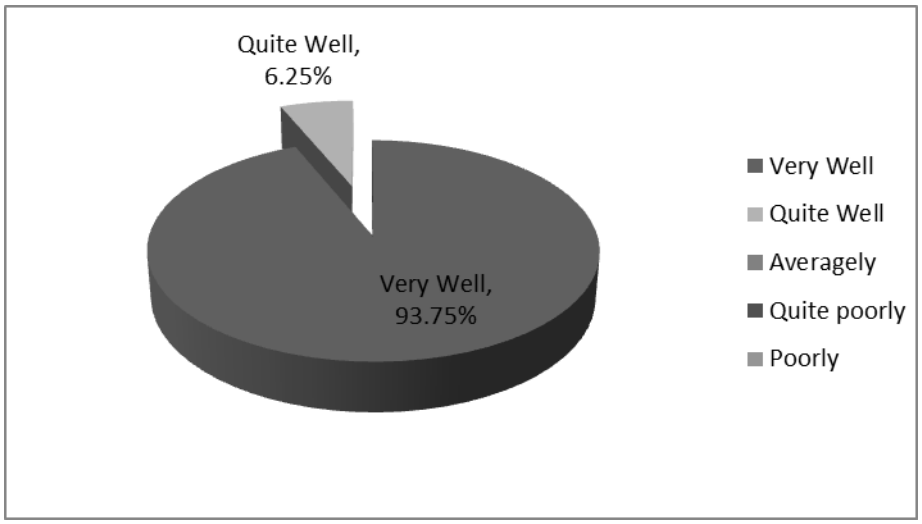
How well were the aims and objectives explained?



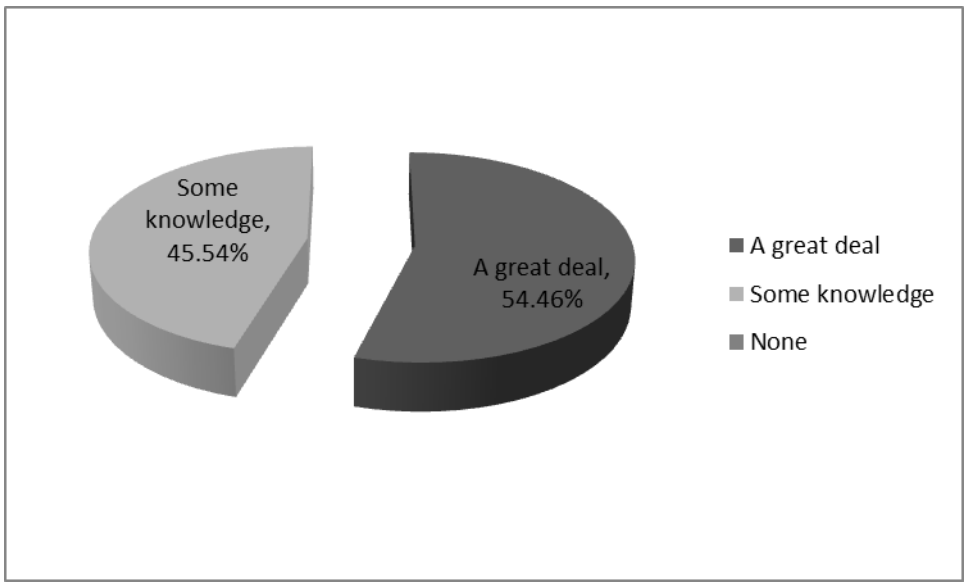
How well did the trainers know the subject?



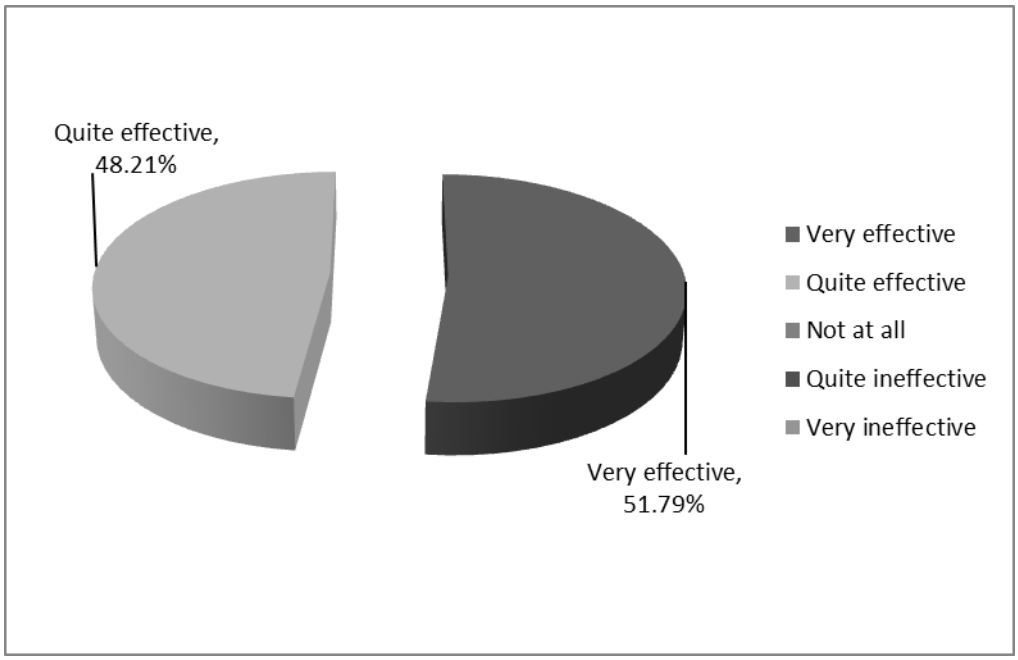
How well did the trainers convey their knowledge?



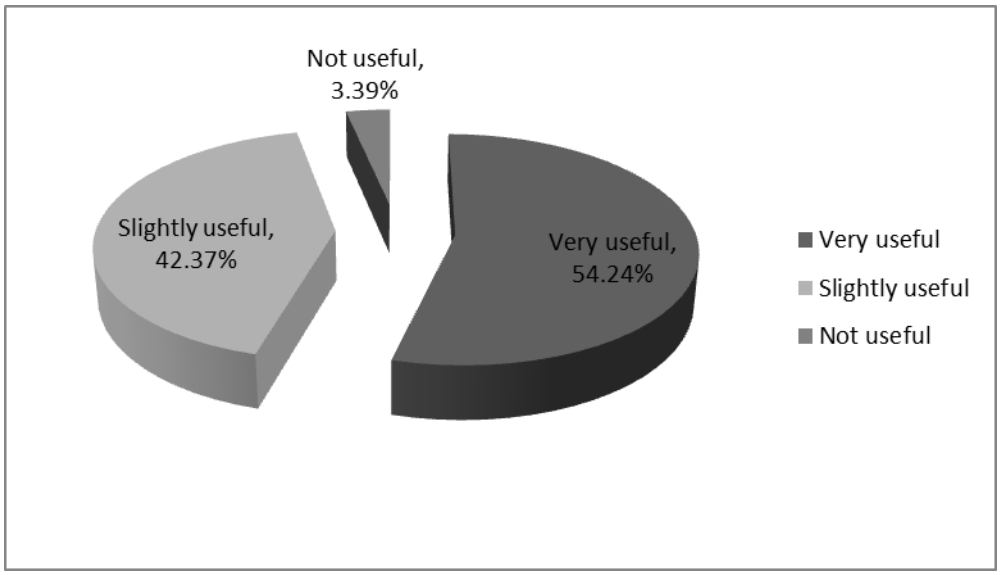
Do you think you learned anything as a result of today?



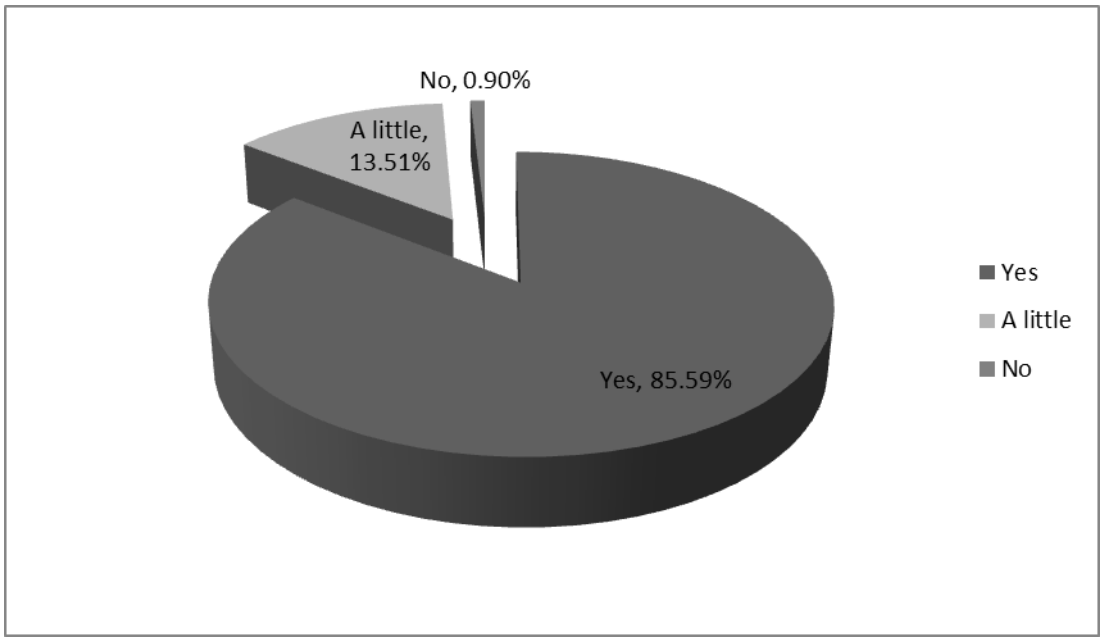
How effective were the presentation materials?



How useful were the group discussions involving the flipchart?

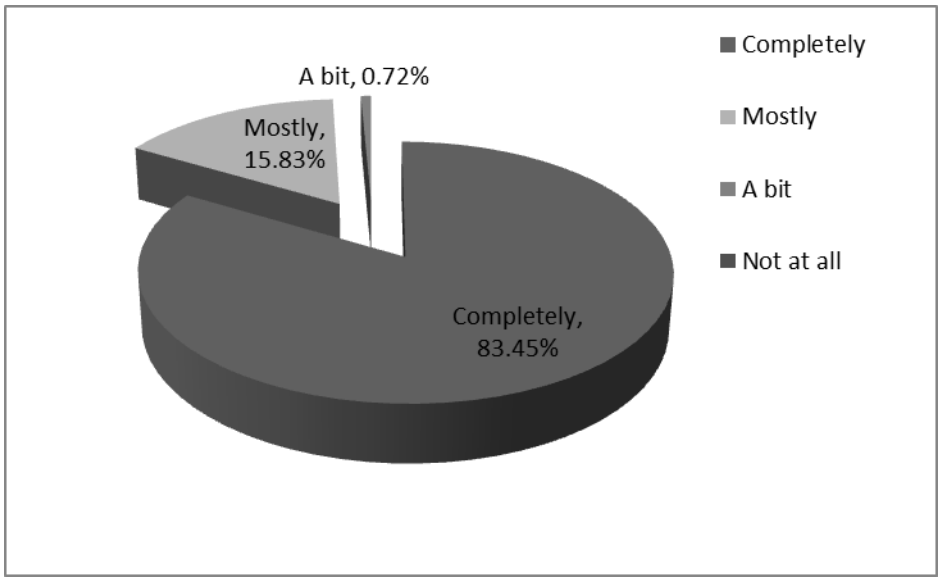


Will you be able to apply any new knowledge gained, in your workplace?

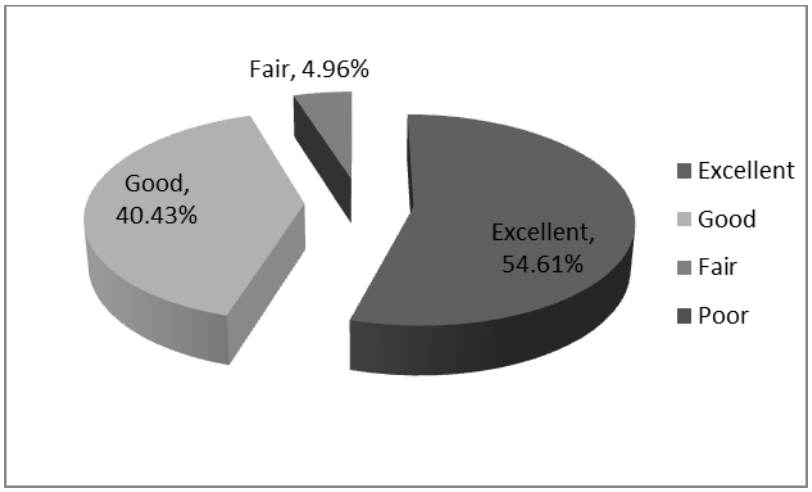


Appendix B - Social Services Training Evaluation 2016/17

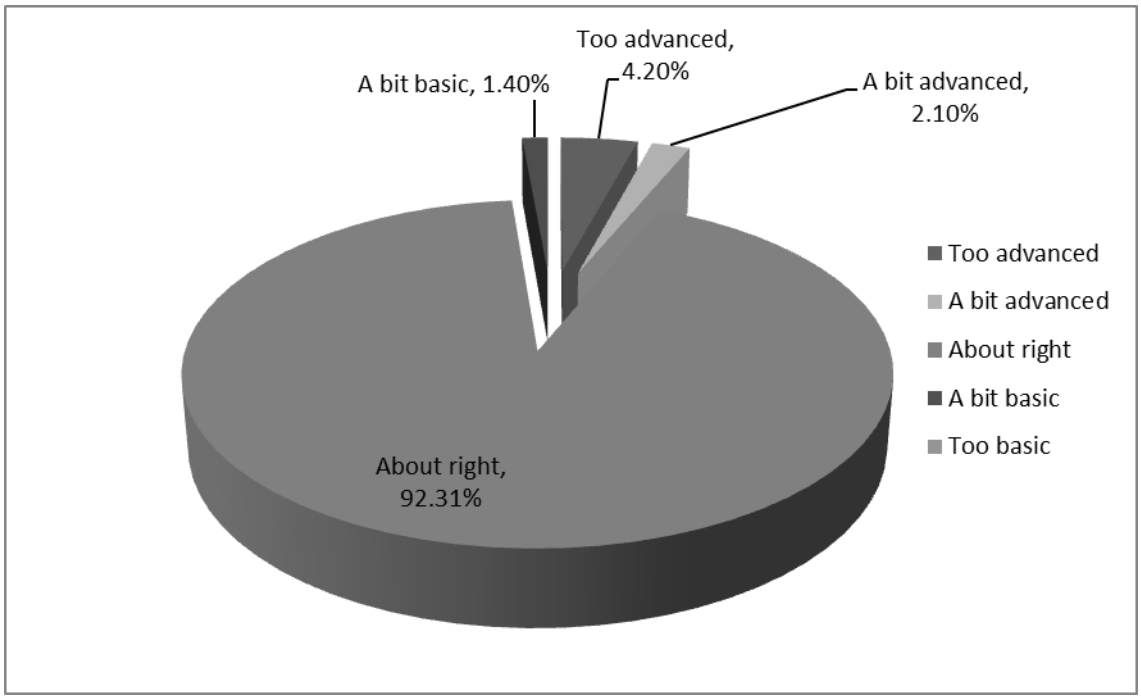
The agreed objectives were met;



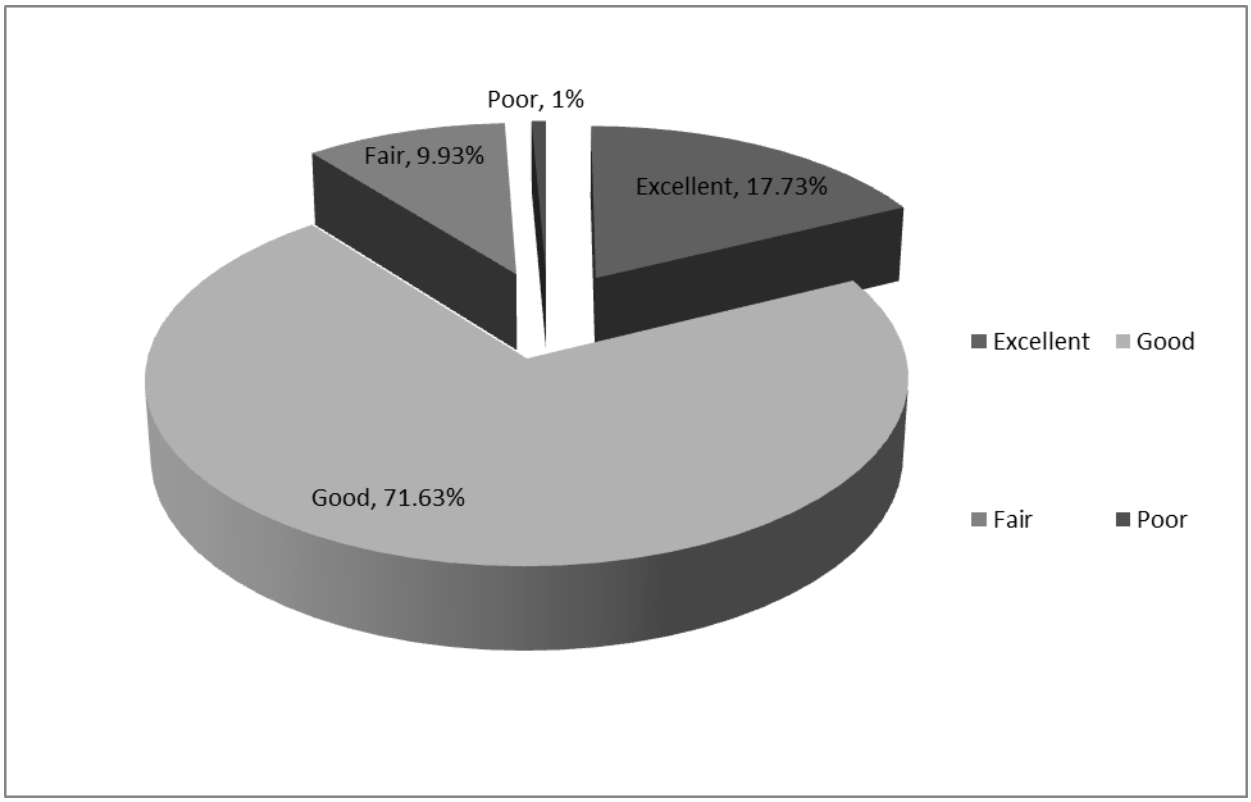
The standard of presentation was;



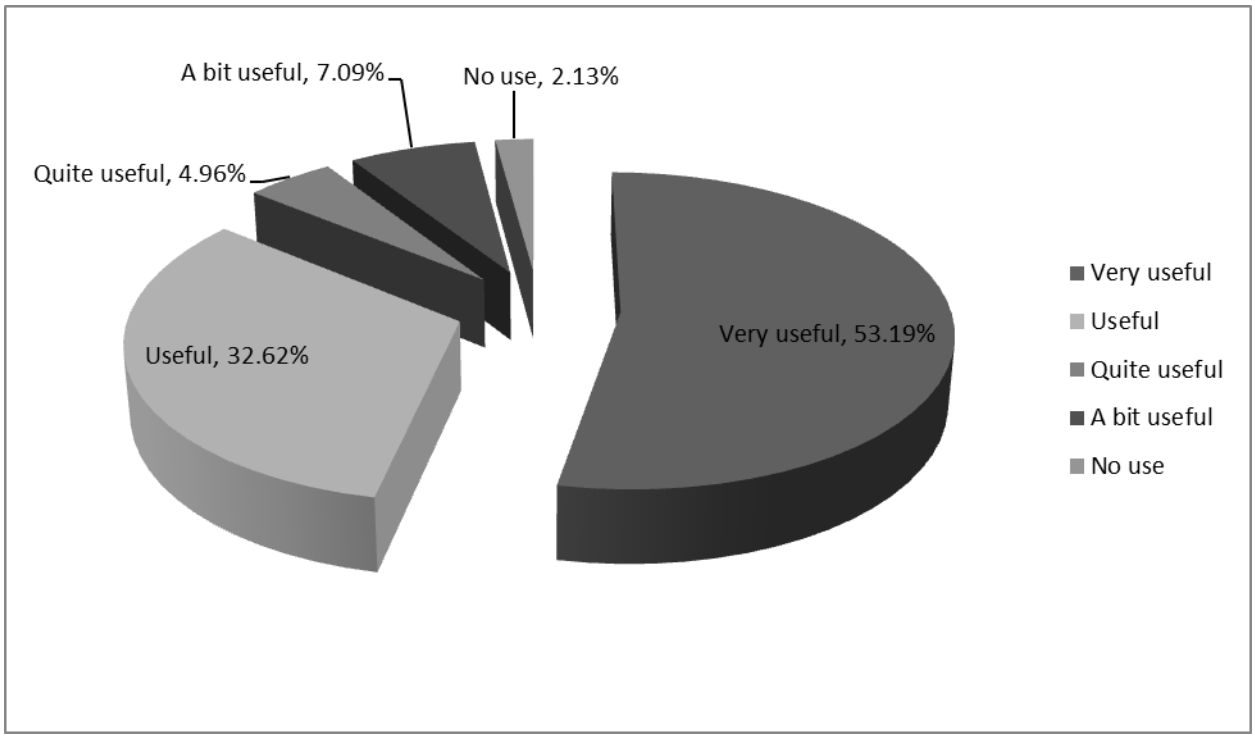
The level of training was;



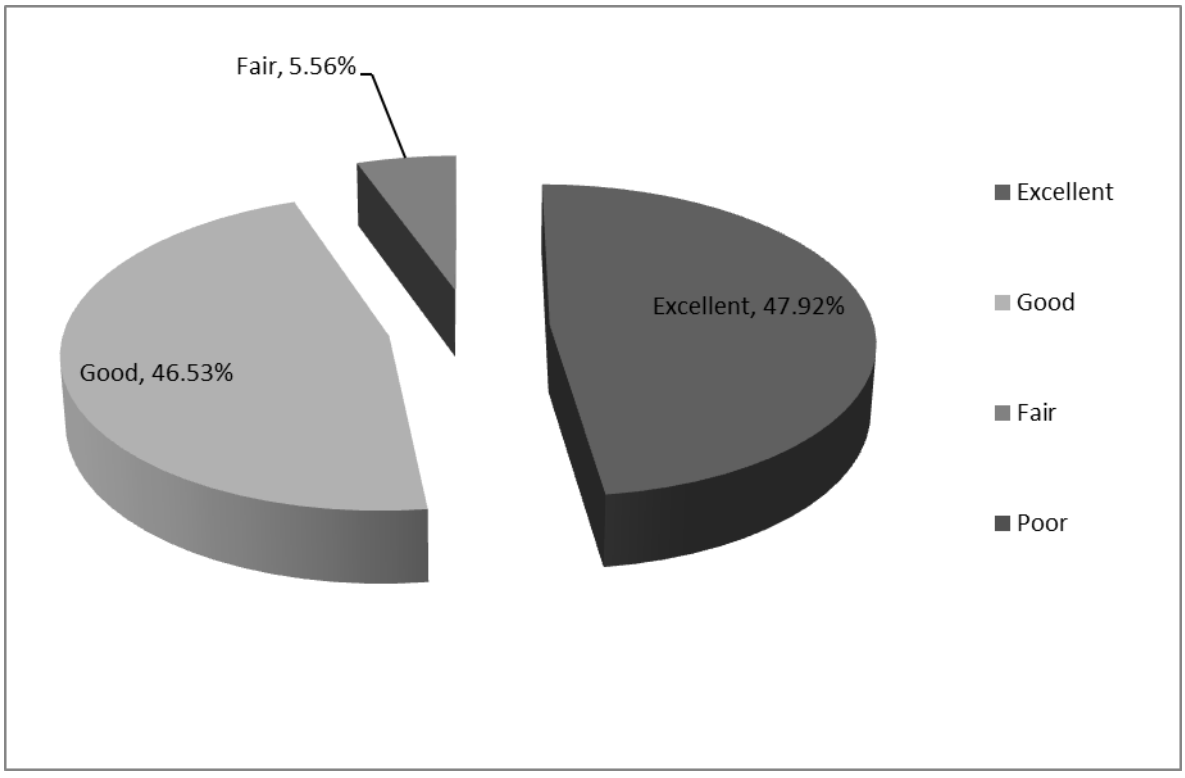
The standard of the venue and facilites were;



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?