Report author: Andrew Nutting
Tel: 07891 276168

Report of Deputy Chief Executive

Report to Corporate Governance and Audit Committee

Date: 18th March 2016

Subject: Annual Information Governance Report

Are specific electoral Wards affected? If relevant, name(s) of Ward(s):	☐ Yes	☒ No
Are there implications for equality and diversity and cohesion and integration?	☒ Yes	☐ No
Is the decision eligible for Call-In?	☐ Yes	☒ No
Does the report contain confidential or exempt information? If relevant, Access to Information Procedure Rule number: Appendix number:	☐ Yes	☒ No

Summary of main issues

1. The work required to address the recommendations of the Information Commissioners Audit report has been completed or is underway. Delivery against the remaining recommendations is being carried out by a small team of Information Governance professionals and completion is expected by March 2017.

2. Significant, strategic work on Information Management and Information Governance is being undertaken to strengthen management of information in support of the business of the council, to respond to external requirements and to identify opportunities for efficiency and other value gains in the management of information.

3. The council is establishing a Cyber Resilience Working Group to deliver against the Government's recently published ten steps to Cyber Resilience and to build on existing control and contingency plans to enable the council to avoid or recovery quickly from any cyber-attack.

4. The council continues to handle and process requests for information in accordance and compliance to appropriate legislation such as the Data Protection Act and Freedom of Information Act.

5. There is a growing risk about the council's ability to meet the INSPIRE Regulation requirements within prescribed deadlines. The issue centres on the council's capability and ability to publish the required datasets. Discussions are progressing about the

development of a corporate capability to manage GIS, which in turn, would provide a focus on INSPIRE work and help to mitigate against risk of non-compliance.

Recommendations

1. Corporate Governance and Audit Committee is asked to consider the contents of this report and the assurance provided as to the Council's approach to information governance.

1 Purpose of this report

1.1 To provide Corporate Governance and Audit Committee with an annual report on the steps being taken to improve Leeds City Council's information governance in order to provide assurance for the annual governance statement.

2 Background information

2.1 Leeds City Council recognises the need to protect its information assets from both accidental and malicious loss and damage. Information Governance is taken very seriously by the council and this is evidenced by the on-going work to improve the management and security of our information as outlined in this report.

2.2 The report provides Committee Members with an update on the more strategic and cross-council activity on-going to provide assurance on our approach to information governance.

3 Main issues

3.1 ICO Audit

3.1.1 Auditors from the Information Commissioner's Office (ICO) visited the Council in October 2013 to carry out an audit of its processing of personal data following enforcement action at the Council in 2012. Whilst, the audit provided the ICO with reasonable assurance about our data protection practices, auditors provided a list of 32 recommended improvements to current practice for the council to implement. Members of this Committee received a detailed report on 21st January 2014 regarding the audit, and a further report was considered on 20th March 2015 outlining progress made to date. Appendix A to this report contains a summary and further update against these recommendations

3.1.2 Work on twenty two of the thirty two recommendations is now complete and actions embedded into information governance standards and/or practice. Of the outstanding ten recommendations work is due to be completed on a further five by 30th June 2016. The remaining five recommendations constitute an investment in some fairly significant work. There is a small core of professional IG officers delivering against these recommendations who are managing delivery of this programme against a backdrop of competing priorities. However, the ICO are no longer monitoring progress, and will only take a further interest should the council be subject to a reportable information incident. The last recommendation is scheduled for completion by 31st March 2017 and the Executive Officer (Information Governance) will continue to monitor progress.

3.2 Overall arrangements for Information Assurance

3.2.1 In line with recommended practice for public authorities in the UK, the Council has established demonstrable arrangements which will ensure that information assurance is addressed along with other aspects of information governance.

3.2.2 The council has an established and fully trained Senior Information Risk Owner, the Deputy Chief Executive, who has overall ownership for information risk management across the council.

3.2.3 The SIRO is supported by the Chief Information Officer who has delegated decision making powers for information governance. The Chief Information Officer chairs the council's Information Management Board which ensures good standard information management practice is embedded into business processes, and information standards and policy are fit for purpose and kept up to date. Decisions made by the Chief Information Officer at the Information Management Board are effectively communicated across each Directorate through their respective Information Management and Technology Team.

3.2.4 The Director for Adult Social Care is the council's Caldicott Guardian. This is a strategic role responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information sharing across Health and Social Care.

3.2.5 A Corporate Information Governance Team with responsibility for information strategy and policy provides support to the SIRO and the Chief Information Officer. In turn this Corporate Team is supported by a range of Information Governance officers across Directorates.

3.2.6 The Chief Information Officer is undertaking a review of how Information Governance is to be delivered across the council in an intelligent, agile, flexible and committed way. This review of the delivery of Information Governance has accepted that there should be an Information Governance Service within the Council and that it should be shaped to face future challenges, including the need to integrate and work with partner organisations in the City.

3.2.7 Significant features of this review include a review of the structure of Information Governance teams across the council and a review of Information Governance policies, and associated procedures and processes

3.2.8 Both the review of the Information Governance service and the review of policies are being undertaken to reflect how the internal and external environment has changed over the past five years, and to take into account use of new 'non-traditional' technologies such as the Cloud, Google Docs and file sharing; provide assurance against new risks to our information assets such as Cyber-crime; and reflect changes to legislation and regulations, such as the EU Data Protection Regulation.

3.2.9 There have been a number of high profile cyber incidents over the last twelve months, including incidents at Ashley Madison, Talk Talk and Lincolnshire County Council. The Council has begun establishing an approach to "Cyber Resilience". Cyber resilience is the capacity an organisation has to prevent, identify and mitigate the impact that a cyber-incident has on the information assets within an organisation. The risk of cyber-attacks has increased from criminals, hackers, hacktivists, terrorists, spies and innocents in the form of phishing, Trojan horses, hacking, stealing, sabotage and prevalent mistakes by employees.

3.2.10 The Government has recently produced guidance on what it calls 'cyber resilience'; this is all about identifying and managing these risks and the persistent threat they present. The guidance recommends ten steps that can help organisations to mitigate or prevent attacks. The Council's Corporate Leadership Team received and considered a report in February outlining where we are in relation to each of the ten steps, along with our improvement plans where needed. Following this, CLT have requested that all senior officers are provided with awareness and information regarding cyber resilience.

3.2.11 Leeds City Council is broadly maturing in its approach to information and to Cyber Security although in certain areas significant work remains to be followed through. To put this in perspective, this hard work is being recognised nationally and LCC were one of a small number of local authorities invited to take part in a cyber-resilience exercise hosted by the LGA; OGSIRO; and, CERT-UK on 20th January. The exercise tested each authority's current capability to respond to a cyber-incident through a series of interactive sessions covering cyber preparedness and the 10 cyber steps. Informal feedback received to date suggests that LCC did well in the exercises.

3.2.12 In order to provide on-going assurance within Leeds City Council, a Cyber Resilience Working Group has been organised to build on existing controls and contingency plans so that the council is able to avoid or recover quickly from such attacks, and to develop plans to further embed necessary actions against the ten steps. This work links with similar work undertaken by other public authorities across the Yorkshire and Humber Region under the auspices of a group known as the Warning, Advice and Reporting Point (WARP). In the event of a cyber-attack a regional response would be invoked proportionally to the circumstance. A chapter on cyber resilience is being included in the revised content for the staff level one mandatory training programme to be launched in June this year.

3.2.13 Information legislation provides rights for citizens to access information held by the council. In respect of the Data Protection Act (DPA) this provides a statutory right for citizens to access information held about them within forty calendar days of submitting a request. Under the Freedom of Information Act (FOIA) citizens have a right to request information held by a public organisation, such as the council, and unless an exemption applies, the council is under a duty to provide this information within twenty working days of receiving a request.

3.2.14 The need to be able to locate and retrieve information is essential, both to enable the council to operate effectively and efficiently and to respond to information requests within the statutory timescales prescribed. The risk to the council of non-compliance would be enforcement action from the Regulator, the Information Commissioner's Office (ICO). The ICO has a range of enforcement actions it can impose, including issuing monetary penalty notices of up to £500,000 for serious breaches of the DPA; the issue of undertakings committing an organisation to a particular course of action in order to improve its compliance (DPA/FOIA); serve enforcement notices and 'stop now' orders on organisations (DPA/FOIA); and, prosecute those who commit criminal offences under the Act (DPA/FOIA).

3.2.15 A team of Information Practitioners ensure that all requests for information to the council are processed and dealt with according to respective legislation and within

statutory timescales, and handle complaints from citizens and enquiries from the ICO. The ICO monitors the performance of all public authorities to ensure that they are compliant with legislation. Therefore it is important the council performs well in dealing with citizens requests for information, and continues to improve information governance practice in information processes, systems and networks to improve access and availability of information. The table below outlines the numbers of requests received and handled by the council for both the DPA and FOIA during 2013/14, 2014/15 and figures to date for 2015/16:

	2013/14	**% compliance to statutory timescale**	**2014/15**	**% compliance to statutory timescale**	**2015/16 to Feb 2016**	**% compliance to statutory timescale**
DPA – Subject Access Requests	453	78.5	466	81.6	394	86.0
FOIA – Requests for Information	2066	93.6	1986	92.9	1476	95.5

3.2.16 There is an embedded Information Security Incident Management and Reporting process across the council, which is coordinated by Information Compliance Officers. Since the Information Commissioner's audit in 2013, the council has a continued improved record and not experienced any incidents which have required involvement by the Information Commissioner. Staff awareness and training on information governance remains an important and integral part of the council's information strategy and is delivered through a series of training programmes. The Level One training is mandatory to all staff, and during 2014/15, over 96% accessed the training programme. Mandatory training is provided every two years, and content for 2016/17 training is being finalised for a launch in June 2016. The ICO recommend regular staff training, as this helps to, not only make staff aware of their responsibilities for information, but mitigate against information incidents. Member Management Committee has recently approved the development of Information Governance training and awareness programme for elected Members so that they understand basic information governance practice around information security and information sharing.

3.2.17 In September 2014 the Government published a new version of the Local Government Transparency Code making it a mandatory requirement to publish named datasets. There are 16 datasets that the council must publish and within each dataset there is mandatory information that must be published. The Code also recommends further information which is optional to publish in addition to the mandatory requirements. The council is fully compliant with the Code as it publishes

all mandatory data, including the new section on Social Housing introduced in September 2015. The council's focus has been on ensuring that it complies with the mandatory requirements. However, when the opportunity presents itself, additional information recommended in Section Three of the Code will be published.

3.2.18 Leeds City Council is required to make all INSPIRE* related data (as is) and metadata available to view and download. This phase should have been completed by December 2013. The council has since procured a software package using funds from DEFRA to enable it to publish the first 'most common' 20 datasets – an approach adopted by many local authorities. From October 2015 any **newly created** datasets should be published to INSPIRE standards – this ensures comparisons of data can be made across all 28 EU Members States. All existing datasets need to be transformed from their current format to exacting INSPIRE standard formats by December 2020.

3.2.19 At present, the council has published 4 of the first 20 datasets. There is an issue around the lack of resources to focus on this work and the absence of a corporate GIS team. There will be a significant amount of work required by GIS users across the council who manage data which may fall under this directive not only to publish it in its current format, but also ensure it is transformed by the 2020 deadline.

3.2.20 Discussions are progressing about the development of a corporate capability to manage GIS, which in turn, would provide a focus on INSPIRE work and help to mitigate against risk of non-compliance.

3.2.21 In 2013 the council was subject to an undertaking by the Information Commissioner in respect of an inadequately drafted contract under which the council required a supplier to process personal data its behalf. The undertaking required the council to embed measures to ensure that all contracts are properly drafted in line with the Data Protection Act when the contracts involve the processing of personal data on its behalf. All council contracts were checked as part of this undertaking and an interim measure was applied wherever required.

3.2.22 The responsibilities and liabilities of the Data Protection Act fall on the council (data controller) to ensure that a supplier processing personal data on its behalf (data processor) does so within the Acts requirements while fulfilling the main contract. This means the contract has to include, where necessary, specific instructions to supplement the terms and conditions. It is a feature of the current Data Protection Act that the data processor is not subject to the Data Protection Act when processing data on behalf of the data controller and is not liable for non-compliance except under contract.

3.2.23 Since the undertaking was issued, comprehensive measures have been designed and put into place. Standard procurement rules were revised in 2013 and they now include instructions and processes for capturing information governance requirements and incorporating them into contracts. Contract management plans are now an obligatory part of the contract preparation process. These measures have been followed through and it was found that staff required further training on some aspects which were difficult to interpret. Advice has now been written and is being delivered in a series of training sessions to all procurement and commissioning staff during spring and early summer 2016. This work will pre-empt

non-compliance by suppliers which may result in harm to an individual and/or financial sanctions on and reputational damage to the council.

4 Consultation and Engagement

4.1 Consultation on the development of strategies, policies, procedures and standards are extensively undertaken across a broad range of stakeholders including information management professionals, representatives from all Directorates via representatives of Information Management and Technology Teams and Information Management Board members.

5 Equality and Diversity / Cohesion and Integration

5.1 Equalities, diversity, cohesion and integration are all being considered as part of delivering the Information Management Strategy. This refers to the way training is being delivered as well as how policies will impact on staff and partners.

6 Council policies and City Priorities

6.1 The policies support the Information Management Strategy and contain areas of legal requirement. Furthermore, the implementation of the Information Management Strategy will improve the quality of the council's policy framework by ensuring the authenticity, integrity and security of the information contained therein.

6.2 Under the Code of Corporate Governance in Part Five of the council's Constitution, the fourth principle (taking informed and transparent decisions which are subject to effective scrutiny and risk management) requires decision making processes and enables those making decisions to be provided with information that is relevant, timely and gives clear explanation of technical issues and their implications.

7 Resources and value for money

7.1 Capacity within Directorates to deliver, embed and monitor compliance to information governance and information risk management practice is been resourced through the implementation of Information Management and Technology (IM&T) teams within each Directorate. Information Governance FTE's are included in each of the IM&T teams.

7.2 The way Information Governance is structured and organised is currently being reviewed with a view to ensuring that the way information management is deployed and delivered across the organisation and city takes account of the Better Business Management Principles: Standardise; Simplify and Share.

7.3 Internal Audit have allocated 60 days each year for Information Governance related audits. In 2014/15 an audit was carried out in relation to some follow up work on the programme of checks on contracts required by the ICO Undertaking issued to the council in 2012. In 2015/16 Internal Audit is undertaking a review of the Information Security Management System (ISMS), producing a control risk assessment and assessing council compliance against it at a high level. This will allow for an audit programme to be developed and will help inform decisions on both future

information governance internal audit coverage and areas of the ISMS requiring attention before a detailed review.

8 Legal Implications, Access to Information and Call In

8.1 Delegated authority sits with the Deputy Chief Executive and Senior Information Risk Owner and has been sub-delegated to the Chief Information Officer under the heading “Knowledge and information management” in the Deputy Chief Executives Sub-Delegation Scheme.

8.2 There are no restrictions on access to information contained in this report.

9 Risk Management

9.1 The risk associated with not implementing information governance policies, procedures and practice across the Council leaves the organisation more susceptible to breaches of legislative, regulatory and contractual obligations, affecting the confidence of its citizens, partners, contractors and third parties when handling and storing information.

9.2 Information risk is being systematically addressed by joining up the approach to risk required by information security standards, the need for the senior information risk owner to be clear about the risks he/she is accountable for and the council’s standard approach to risk management.

9.3 Further work is being undertaken in conjunction with the Corporate Risk Manager to embed the recording and reporting of information risk monitoring and management. The Information Asset Register exercise will generate information required and an automated dashboard will be produced to report risk assessments to the SIRO. This will provide the assurance required by the SIRO from the business and will allow risk mitigations to be prioritised.

10 Conclusions

10.1 The work of the previous year, reported to this Committee on 20th March 2015, has been continued.

10.2 The establishment of information governance practice and procedures outlined in this report provides a level of assurance to Committee that the range of information risk is managed both in its scope and through to service delivery. It allows the council to work with partner organisations, third parties and citizens in a clear, transparent, but safe and secure way. It helps to protect the council from enforcement action and mitigate the impact of cyber incidents aimed at attacking and/or bringing down council information systems.

11 Recommendation

11.1 Corporate Governance and Audit Committee is asked to consider the contents of this report and the assurances provided as to the Council’s approach to information governance.

Background documents1

[1] The background documents listed in this section are available for inspection on request for a period of four years following the date of the relevant meeting. Accordingly this list does not include documents containing exempt or confidential information, or any published works. Requests to inspect any background documents should be submitted to the report author.

Appendix A

Leeds City Council actions against recommendations made by the Information Commissioner

No	Recommendation	Current position as at February 2016	Status	Completion
1.	A6. Ensure IAOs are trained in line with proposed plans. Further advice on IAO training is available from The National Archives.	Council's Corporate Leadership Team has approved the nomination of Information Asset Owners who will be responsible for managing information risk within their services and ensuring compliance with internal policy and external regulatory requirements. A Project plan has been developed and approved by the Information Management Board to refresh the Information Asset Owner role and to provide a full engagement programme to train IAIO's and support staff. A digital database has been developed and tested for use by IAO's to record their information assets, and thereby automate the Information Asset Register. A training and engagement programme has been developed. Resources now deployed and work is currently under way in Environment & Housing And Adult Social Care to create a Register by 30th June. Work is expected to begin in remaining Directorates through the course of this year.	Partially Complete	31 December 2016
2	A10. It would be advisable to have a permanent resource	Training Officer now in place	Complete	

	within the IG Team to ensure that this essential training is developed, maintained and delivered over the long term.			
3	A11. Members of the IG team should be suitably qualified to enable them to carry out their role effectively. It would therefore be advisable for the Council to provide relevant professional training.	Work has begun on a staff competency framework and workforce development plan, which will include IG requirements for IG staff. The competency framework is based on IM&T service functions and strategy and will be aligned to career families. It will identify competency/skills gaps; build competency frameworks into staff appraisals; exploit cross-service coaching, mentoring and training opportunities; and recognise qualification requirements. The staff competency framework work is linked in with the ongoing review of Information Governance Service across the council.	Partially Complete and Ongoing	31st December 2016
4	A12. To comply with the Local Public Services Data Handling Guidelines, the Council should provide suitable CESG training for the ITSO.	Training now completed	Complete.	July 2015
5	A13. The Council should ensure regular IG refresher training is mandated and monitored to ensure staff knowledge is kept up to date and relevant.	Regular mandatory IG refresher training is provided to all staff every two years. The latest refresh was in 2014 and more than 96% of staff have undertaken the training. New content is being finalised for the second version of the IG refresher training to be launched in June 2016.	Complete. Actions Ongoing.	Embedded practice every two years.
6	A21. Provide digital key safes for use within social services	Adult Social Care and Children's Services Directorates have refreshed their practices around	Complete	June 2015

	teams to ensure that records are always accessible when required.	the storing and accessing of records and the implementation is being monitored. Environment And Housing are adopting the same practices		
7	A22. Provide a lockable storage solution for social workers taking manual personal records off site on client visits, such as lockable document holders, bags and/or car boot safes.	Adult Social Care and Children's Services Directorates have refreshed their practices around the storing and accessing of records and the implementation is being monitored. Environment and Housing are adopting the same practices.	Complete	June 2015
8	A23. Introduce a standard procedure for signing files out of the office and ensure the file returns are monitored.	A new corporate standard and procedure for tracking and tracing of files has been developed and agreed and is currently being implemented .	Partially Complete	30 June 2016
9	A27. Regularly monitor boxes and files which have been removed from the RM storage facility to ensure files are returned in a timely manner and enable the early identification of any missing records.	Current processes enable the movement of records that are within the control of the corporate records management facility to be tracked and traced although a new process containing improvements is about to be installed. The new database (Phase One E-workplace Programme) is likely to be deployed by 31st May 2015 that will address this issue.	Complete	31 Dec 2015
10	A28. Ensure all visitors to office buildings containing sensitive personal data are recorded in a visitor's book and ensure codes for doors with pin code access are regularly changed and this is recorded.	In a review of buildings from which council services operate, 21 high risk buildings were identified and 25 medium risk. A small core team of IG professionals began auditing in 2015 and have now completed audits of 17 of the high risk buildings and 15 of the medium risk. Auditing continues of the remaining high and medium risk buildings. During the audit the procedures relating to visitors have been reviewed and updated where necessary.	Partially Complete	30 June 2016

		Further work on other council buildings deemed low risk is to be carried out by Directorate IM&T teams throughout 2016.. .		
11	A29. Implement a procedure for routine spot checking of compliance with the clear desk policy.	A plan to introduce routine spot checking for staff compliance with the council's Clear Desk/Clear Screen policy has been developed and implemented based on annual routine s	Complete and procedure on-going.	30 April 2015
12	A30. Ensure all manual records containing personal data are locked away at the end of the day.	Revenues and Benefits have provided lockable cupboard in visitor office and have provided assurances paperwork containing personal data is locked away at the end of the day.	Complete	
13	A37. Wherever available ensure that follow me printing is enabled. For devices which do not have follow me capabilities, introduce a system of spot checks to ensure information is not left on printers for any longer than necessary.	A new contract for Print Services across the council was awarded to an external contractor in July 2014. PIN printing was a default requirement in the contract specification. Contract has been rolled out in full.	Complete	31 October 2015
14	A39. Ensure that the protective marking scheme is implemented as soon as is practicable.	The requirement on Local Authority's is unclear and advice has changed at a national level. The full requirement appears to be narrower than originally envisaged. Where the requirement is clear this has been implemented. Clarification is being sought on the remainder of the requirement. The actual implementation of this appears to be unlikely to be acceptable/feasible/cost effective within Leeds City Council at the current time.	Complete	31 July 2015

15	A42. Ensure that the retention schedule is finalised and implemented as soon as is practicable.	The retention schedule is now complete and signed off by Legal Services and is now in use across the council.	Complete	30th June 2015
16	A44. Ensure that offices which are using unsecured confidential waste bags are provided with the standard lockable containers which are part of the confidential waste contract.	The council developed an action plan to deliver against recommendationsA28, A44 and A46. An audit of buildings has taken place and we have a better understanding of the off-contract position across the council. Issues uncovered have been and will be dealt with as part of that exercise which is now moving towards completion The plan is now, in combination with work to deliver against A28 and A46, to issue a questionnaire to buildings managers to identify current practice in relation to use of shredders and alternative confidential waste providers and to work towards moving these onto the council's confidential waste contract. The aim is to deliver against this action	Partially Complete	30 June 2016

		plan by July 2016.		
17	A46. Carry out an audit of shredders and consider the introduction of cross-cut shredders for sensitive personal data, or the use of locked confidential waste bins with subsequent secure in-house or third party destruction.	As per A 28 & A44.	Partially Complete	30 June 2016
18	A47. Ensure ESCR files transferred to new casework systems are appropriately weeded in line with the Council's retention schedule.	The weeding process has been completed and has been transfered to the new system	Complete	June 2015
19	A48. Ensure that RM KPIs are routinely communicated to appropriate boards, including IGMB, from relevant sub groups.	KPIs have been agreed by IMB and a dashboard for reporting initially to IMB has been built	Complete	30 April 2015
20	A49. Establish suitable RM KPIs for all directorates and ensure these are appropriately reported within the IG structure.	Key Performance Indicators have been developed and, following a formal consultation process with key stakeholders, approved and included in the Information Services Service Plan 2014/15.	Complete	
21	A51. Ensure that PIAs are embedded across the Council at the implementation stage of any projects involving the processing of personal data.	There is a new framework for the delivery of projects and programmes and also contracts and contract management. Council PIA's to be implemented as part of the process. The use of PIA's has been mandated by IMB. Training in their use in contracts has been organised for delivery by the end April 2016 and then	Partially Complete	31st December 2016

		cascaded and a guidance resource on InSite is in production. This will then be updated for project and programme management methodology.		
22	B4. Formalise a process for ensuring IG KPIs are reported to the IGMB from its sub-boards and these are recorded and formally reported back to both the SIRO and the Risk and Performance Board and/or Internal Audit.	Key Performance Indicators have been agreed by IMB and a dashboard for reporting to IMB has been built. The SIRO is appraised throughout the year through monthly meetings with the Executive Officer (Information Governance).	Complete	5
23	B6. Consider making the IT Security Officer a permanent member of the IKM /ICT Liaison Group so there is a clear reporting line to the SIRO, as recommended in the Local Public Service Data Handling Guidelines.	The IT Security Officer was made a member of the ICT/IKM Liaison Group. However subsequent to this, The Corporate Information Governance Team have moved under the management of the Chief Officer for ICT (Chief Information Officer). As such the Executive Officer (Information Governance) now sits on the Management Team and all IG/IT issues are shared at this forum. Following this reorganisation, the ICT/IKM Liaison Group has been disbanded. Furthermore, the Executive Officer (Information Governance) and the IT Security Officer now report to the same Head of Service, which has strengthened collaboration between the two areas on matters relating to PSN Connectivity, IG Toolkit, and Information Security policy .	Completed	1st April 2014
24	B13. Ensure a formal information security risk assessment and management programme for all information assets on the Information Asset Register has been documented, is implemented by Information Asset Owners and regularly monitored and	See action 1 above Preparation work is underway with the Corporate Risk Manager and a dashboard will be required to consolidate risk assessments to provide "heat maps" at various level of the council. It will also act as an action tracker at service level.	Partially Completed	31 March 2017

	reviewed.			
25	B15. Ensure on-going IG work continues to address actions identified in the 2011/12 Internal Audit follow-up review of the effectiveness of the IG team.	A review has been undertaken of the 2011/12 Internal Audit actions, and those recommendations not completed have been accommodated into the Corporate IG Team Work Programme for 2014/15 – February 2014.	Completed	1st April 2014
26	B17. Ensure the cover sheet of all IG polices is completed with the latest review date.	Undertaken in December 2013	Completed	31st December 2013
27	B18. Ensure the ISP is linked to the relevant suite of IG policies to ensure staff are clear which policies are associated with it.	Undertaken in December 2013.	Completed	31st December 2013
28	B26. Continue the review of all Council contracts to ensure that data protection requirements are appropriately specified within them.	Work with the Public, Private Partnership and Procurement Unit to embed information governance checks and balances into the Corporate Contract Framework is complete. Training is being developed and rolled out to all staff involved in contract activity. This is now complete and appropriate information is now being included in all contracts.	Partially Completed.	30 April 2016
29	B32. Review password access to all databases to ensure they comply with enforced change and complexity rules as required by the password management policy.	The Council has done considerable work to locate databases and to confirm the access route(s) to them. The majority of databases utilise access routes that require users to logon to the council or device in a manner that complies with the council password management policy.	Complete	1st March 2015
30	B34. There is a risk that staff who have moved departments	The council's HR function has information of staff who move internally. Possibilities of exploiting SAP	Partially Complete	31 October 2016

	within the Council are not promptly removed from access to databases containing personal data which they no longer require. Ensure HR provide systems administrators with a list of staff who have moved departments to cross reference against staff access rights.	have been explored and although part of the requirement can be implemented this way for leavers, internal transfers cannot. Manual HR procedures will now be looked at a Policy level and via a newly formed Cyber Essentials Working Group.		
31	B44. Review the risks of laptop users being able to save data to their local C drive. This unstructured data is not automatically backed up and therefore may not conform to Council retention policies and is not searchable for information requests.	A review has been undertaken and a solution defined which addresses this problem. A Microsoft product which synchronises data from local hard drives to personal space on the shared drive has been employed and access permissions re configured to allow this to work. Data saved on a laptop is not backed up and may be lost. When synchronised to the shared drive it is backed up. This measure also prevents confusion between versions of documents.	Complete	31st December 2015
32	B48. Ensure staff storing personal data at home are provided with a secure lockable cabinet as detailed in the Remote Working Policy.	Remote Working Policy has been reviewed and now ensures that this happens.	Complete	31st December 2015