CYNGOR SIR YNYS MON / ISLE OF ANGLESEY COUNTY COUNCIL	
MEETING:	**AUDIT & GOVERNANCE COMMITTEE**
DATE:	**21 September 2016**
TITLE OF REPORT:	**INFORMATION GOVERNANCE – SENIOR INFORMATION RISK OWNER'S ANNUAL REPORT FOR 1ST APRIL 2015 – 31ST MARCH 2016**
PURPOSE OF THE REPORT:	**To Inform Members as to the Level of Compliance and Risk**
REPORT BY:	**SIRO/Monitoring Officer** **Ext. 2586 lbxcs@ynysmon.gov.uk**
CONTACT OFFICER:	**SIRO/Monitoring Officer** **Ext. 2586 lbxcs@ynysmon.gov.uk**

1. Purpose of this report

To provide the Audit and Governance Committee with the Senior Information Risk Owner's analysis of the key Information Governance (IG) issues for the period 1 April 2015 – 31 March 2016 and to summarise current priorities.

2. Introduction

This report provides an overview of the Council's compliance with legal requirements in handling corporate information, including compliance with the Data Protection Act 1998; Freedom of Information Act 2000; Regulation of Investigatory Powers Act 2000 (Surveillance) and relevant codes of practice.

The report also includes assurance of on-going improvement in managing risks to information during 2015-2016; and also identifies future plans. It reports on the Council's contact with external regulators and provides information about security incidents, breaches of confidentiality, or "near misses", during the relevant period.

As SIRO the author is not yet able to provide a comprehensive assessment of the Council's level of information risk, and the controls in place, known as a Statement of Control, for the reasons described in this report.

3. Background

IG is the way organisations process and manage information. In its broadest sense, the term covers the whole range of corporately held information, including financial and accounting records, policies, contracts etc. However, for the purpose of this report, IG is defined as how the Council manages and uses *personal information*; that is information about people, be they service users or employees.

Sound IG provides assurance that the way we deal with personal information is effective, lawful and secure. Legislation places a responsibility on the Council to keep personal information safe and IG provides a means to respond if the security of personal information is compromised.

4. Information Governance at the Council

The Council collects, stores, processes, shares and disposes of a vast amount of information. Specifically, though, holding and using information about people includes inherent risk of loss, damage or inadvertent disclosure. Personal information is also expensive to gather, use and hold, and, when things go wrong, it is expensive to replace. It follows that it should be managed as efficiently as all other valuable Council assets, like people, business processes and infrastructure.

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 main statutory driver is the Data Protection Act 1998; significant breaches of which may result in large monetary penalties, currently up to a maximum of £500k. Additionally, if data about individuals is wrongly shared or disclosed, thereby causing them harm (distress and/or tangible damage) they are entitled to compensation.

It is useful to explain at this point that a considerable amount of audit work, including that of the Information Commissioner's Office (2013-2014) has highlighted deficiencies in the Council's data protection arrangements. Since 2013, the Council has invested in improving its compliance with the Data Protection Act and now has in place the relevant policies and procedures to support compliance with the Act.

It is considered good practice to have a SIRO to provide direction and leadership at a senior level. This role is undertaken here by the Head of Function (Council Business) and Monitoring Officer. In order to address information risk, a **Corporate Information Governance Board** (CIGB) was established in November 2014, chaired by the SIRO. This Group is an appropriate forum for addressing IG issues. It receives reports on how well each Service is performing in key information management areas. It assesses risk, and recommends and monitors remedies to mitigate risks to information assets owned by the relevant Heads of Service. The CIGB may report matters directly to the Council's Senior Leadership Team.

Other IG roles within the Council include:

- **Corporate Information Governance Manager**
- **Corporate Information and Complaints Officer**
- **Information Asset Owners** - Heads of Service who '*own'* the assets and are responsible for making sure their information assets properly support the business, and that risks and opportunities connected with it are monitored and acted upon (included within revised job descriptions);
- **Information Asset Administrators** – nominated officers who ensure that policies and procedures are followed, recognise actual or potential security incidents, and maintain the information asset registers (included within revised job descriptions);
- **Internal Audit**

5. Key Organisational Information Risks and Controls

The SIRO cannot report on the adequacy of the controls and mitigations of information risk currently associated with each critical asset. This is because the Council does not yet have a complete understanding of the information risks and the mitigations and controls in place.

However, much progress has been made to develop awareness about information risk and to introduce mechanisms to manage the risk.

The Council has identified risks around information in its corporate and service risk registers.

The Council recognises that harm and distress to individual(s), financial penalties, enforcement action, adverse publicity, and loss of confidence in the Council are risks associated with its information assets.

The Council also recognises the following risks to the security of its information:

- **negligence** or **human error**;
- **unauthorised** or **inappropriate access**, including processing confidential personal data without a legal basis;
- **loss** or **theft** of information or equipment on which information is stored;
- **systems** or equipment **failure**;
- unforeseen circumstances such as fire, flood and other environmental factors;
- **inappropriate access**, viewing information for purposes other than specified / authorised;
- **unauthorised access**, using other people's user IDs and passwords;
- **poor physical security**;
- **inappropriate access controls** allowing unauthorised use;
- **lack of training** and awareness;
- **hacking** attacks;
- '**blagging**' offences where information is obtained by deception.

In addition to technical and physical measures to protect the Council's information, the following main technical and organisational safeguards are in place against information risks:

- suitable **IG Policies** and procedures;
- a preliminary **Information Asset Register**;
- suitable **data protection training** provided to staff on a rolling basis;
- **encrypted ICT** equipment;
- appropriate **service level lessons learnt logs**;
- **data security incident recognition and reporting procedures**, including an investigation and incident-severity analysis methodology;
- **IG KPIs** are gathered and reported to the CIGB every quarter;
- appropriate **IG key roles** identified, designated and trained;
- Council **services are procured** in a data protection compliant way;

- participation in the Welsh Government's **Accord on the Sharing of Personal Information** in order to ensure that sharing of personal data is lawful and proportionate.

Some of the most important issues above are discussed in greater detail below.

5.1 Information Asset Register

The Council's CIGB has developed the first version of the Council's Information Asset Register. An Information Asset Register is the key mechanism for understanding an organisation's information holdings and the risks associated with them. The register allows the mapping of information content and information systems as they interact with changes to business requirements and the technical environment.

The Council's Information Asset Register is not yet developed to the extent that adequate information about the risks to the assets is captured at a granular level. However, development work to identify the main risks associated with each of the Council's business critical systems and assets is tabled for this year; it is intended that this work will be a significant feature in the SIRO's report for the period 2016-2017. It is likely that Services will require corporate support to improve their Information Asset Registers. As this will have to be achieved within existing resources, it will be done on a rolling basis and according to risk; which will be assessed on past and current performance and the sensitivity of the material held by each Service.

5.2 Key IG Policies and Governance

Policies are a key safeguard and are an important element in the Council's IG arrangements. The Council's Heads of Service, in their roles as IAO's, have a singular role in embedding and maintaining policies around the use and handling of information which will improve the quality and consistency of information management across the Council.

The following key IG policies are available on the Council's intranet. The policies are reviewed and updated by the CIGB. This work is timetabled and will always be subject to ongoing review.

- Data Security Incident Policy
- Data Protection Policy
- Clear Desk Policy
- Records Management Policy
- Personal Data Classifications Policy and Guidance Notes
- Access to Information Policy
- Privacy Impact Assessment Policy
- Information Risk Policy

The Clear Desk Policy, Records Management Policy, and Data Classification Policy are mandatory policies for acceptance by the Council's staff. This ensures that employees are clear what the Council's expectations are.

5.3 Policy Acceptance

The link between policy acceptance (i.e. system to evidence training, understanding and implementation) and good practice in data protection is clear. The ICO highlighted this element in his 2013 audit report, and again in 2015, when the Council was asked to ensure that it had procedures for gathering, collating and demonstrating that its staff had accepted key policies. It was also a recommendation from Wales Audit Office in their Annual Improvement Report of 2014-15 dated 1st December 2015.

Funding having been identified, the Council has now procured, and is currently implementing, a policy management system which will provide the SIRO with assurance that key IG policies are being read, understood and formally accepted by individual members of staff. Initial corporate training on this new system was completed on the 12th July 2016. (The policy management system will be of wider application and is the subject of a recent paper to the Heads of Service).

Update June 2016

5.4 Privacy Impact Assessments

Privacy impact assessments (PIAs) are a tool to help organisations identify the most effective way to comply with their data protection obligations. An effective PIA will allow organisations to address problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.

Conducting a PIA is not currently a legal requirement of the Data Protection Act 1998, nonetheless it will become compulsory as part of the new legislation that will come into force in May 2018 (unaffected by the recent EU Referendum decision). The ICO may ask an organisation whether they have carried out a PIA. It is often the most effective way to demonstrate how personal data processing complies with the DPA.

It is necessary for PIAs to be undertaken when a project is being considered, or some new variation of an activity will result in using personal data in a different way; completed PIAs are sent to the Corporate Information Governance Manager.

During the period of this report only one PIA was completed. This is likely an area of compliance that must be improved. There is reason for scepticism about the reliability of this information. To address this suspected non-compliance, ICT project managers are now tasked with flagging intelligence of new systems or changes to existing business practices involving people's information.

5.5 Training

Training provides the Council with assurance that its staff appreciate the requirements of the Data Protection Act as it affects them and the Council's service users. This is important, as the level and adequacy of training is a safeguard against data security incidents occurring and also mitigation if an incident must be reported to the Information Commissioner.

The Council's corporate IG training involves a mandatory basic training for all staff which is refreshed every two years. This training commenced in June 2014 and a process to ensure maximum take up was followed. Processes are in place to ensure that new starters take the training.

5.6 Personal Data Flows and Information Sharing

In addition to maintaining Information Asset Registers, IAOs are required to understand and document data flows in and out of the organisation. This is largely done by means of the Wales Accord on Sharing of Personal Information (WASPI) information sharing protocols, which are good practice and a means of identifying whether information is being transferred outside the UK and EEA, contrary to the Data Protection Act 1998. WASPI information sharing protocols (ISPs) identify risks to the security of information and mitigations that are in place.

ISPs under development during the period of this report are highlighted in **Appendix A**.

5.7 Data Security Incidents

The Council's IG arrangements comply with the Information Commissioner's Guidance on reporting data security incidents that breach the Council's statutory duty to protect personal data.

The Council has therefore established a Data Security Incident Methodology for identifying, investigating and reporting data security incidents. A corporate log is maintained and service logs are also in operation. Additionally, the Council has developed a tool for assessing the severity of data security incidents. The tool enables the SIRO to assess, in 3 steps, the severity of a data security incident by attributing weight to specific factors relating to the scale and sensitivity of incidents. Incidents are scored as Level 0, Level 1, or Level 2.

- **Level 0** are categorised as near-misses.
- **Level 1** confirm data security incident but **no** need to report to ICO and other regulators.
- **Level 2** confirm data security incident that **must** be reported to ICO and other regulators (as appropriate).

The number of incidents recorded by the Council is provided in **Appendix B.**

5.8 Audit Work

The Council's Internal Audit Service has an annual programme of work which includes elements of IG. The CIGB works closely with the Internal Audit Service to provide specific assurance on IG issues, such as testing and compliance with key policies; notably the Clear Desk Policy.

In 2015, Internal Audit completed a comprehensive audit of the Council's IG arrangements. The audit found that the Council's arrangements for IG, risk management and/or internal control were **reasonable**. The conclusions of the Internal Audit report are

not incompatible with the fact that the Information Commissioner issued a formal Enforcement Notice against the Council in October 2015. The Enforcement Notice related to historic issues that the Council is still addressing.

5.9 IG Key Performance Indicators (KPIs)

The Council monitors specific IG KPIs; some on a monthly, and others on a quarterly, basis. It also publishes its access to information data on its website on a quarterly basis.

Information about the number of Freedom of Information Act 2000 complaints investigated by the Information Commissioner is provided in **Appendix C**.

In addition, the Council also holds Internal Reviews of its responses under FOIA at the request of complainants; information is provided in **Appendix D**.

The Council also investigates complaints made to it about data protection matters; further information is provided in **Appendix E**.

Subject access, the fundamental right under the Data Protection Act 1998 to access one's own personal information, is an important element of IG. Subject Access Requests are often complex and resource intensive. Information about the number of Subject Access Requests and the Council's compliance is provided in **Appendix F**.

6. Regulatory Oversight

Oversight of aspects of IG is provided by a number of regulators, reflecting the legislation and codes of practice which relate to the issue. The Council is required to routinely report to the regulators on a number of issues and, where required to do so, on an ad-hoc basis, in respect of certain matters.

It is evident that regulators provide the Council with important feedback on its compliance with statutory requirements, which in turn informs the SIRO's evaluation of IG.

6.1 Information Commissioner

The Information Commissioner is responsible for enforcing and promoting compliance with the Data Protection Act 1998 (the DPA) and the Freedom of Information Act 2000. Section 51 (7) of the DPA contains a provision giving the Information Commissioner power to assess any organisation's processing of personal data against current standards of 'good practice', with the agreement of the data controller.

The Council was required to sign formal Undertakings with the Information Commissioner in 2011 and 2012. The Council, following a significant number of data security incidents, it was audited on a consensual basis in 2013- (with a follow up audit in 2014). The ICO issued its report in 2013 which contained a number of recommendations. The Council established a Corporate Information Governance Project Board to formulate and deliver an Action Plan to implement the required improvements. Almost a 100 agreed objectives had been fully realised by the time of the re-audit by the ICO in 2014.

The follow up audit report by the ICO in January 2015 reduced the Council's risk rating from 'red' to 'amber', and removed the Council from the ICO's formal monitoring

category. Therefore, whilst the re-audit recognised improvements on the earlier findings, an additional 66 activities were required by the ICO. In November 2014 the Council established the CIGB, as a vehicle for delivering the second Action Plan (consolidated CIGB IG Action Plan), arising from the re-audit. These included short and medium term objectives followed by ongoing oversight and responsibility for data protection compliance.

On the 1st October 2015, the ICO issued an Enforcement Notice under the Data Protection Act 1998. The Commissioner concluded that the Council had contravened the Seventh Data Protection Principle by failing to: 'take appropriate security measures against the unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data'. The issues highlighted in the Enforcement Notice's nine recommendations are now the subject of a third Action Plan, devised by the CIGB, and being implemented by a sub-group of the CIGB. Work and resources have had to be reprioritised to ensure that the activities that would best defend the Council in the event of a further reportable data security incident, are completed first.

The Enforcement Notice Action Plan contains 41 actions which are required to implement the nine recommendations. Progress with the nine headings of the Enforcement Notice Action Plan is summarised in **Appendix G.** Work on the consolidated CIGB IG Action Plan, which was displaced by the need to address the Enforcement Notice, will resume once the Enforcement Notice Action Plan is implemented. The CIGB IG Action Plan is summarized in **Appendix H.**

6.2 The Office of Surveillance Commissioners

The Office of Surveillance Commissioners (OSC) oversees the conduct of covert surveillance and covert human intelligence sources by public authorities in accordance with the Police Act 1997 and the Regulation of Investigatory Powers Act 2000 (RIPA). The RIPA regime aims to ensure that directed surveillance is carried out in a manner which is compliant with human rights. This is achieved through a system of self-authorisation by senior officers who have to be satisfied that the surveillance is necessary and proportionate; the self-authorisation must then be judicially approved.

During the year, a number of changes were identified internally and implemented in order to improve the Council's arrangements for compliance with RIPA, in readiness for the OSC audit. The improvements were:

- the SIRO was formally designated as RIPA Senior Responsible Officer;
- the Corporate Information Governance Manager was designated the Council's RIPA Coordinator;
- the RIPA Policy was revised;
- two new corporate registers were created;
- practitioner resources were collated and placed on a new, dedicated page on the Council's intranet site;
- role appropriate training was provided during the year to enforcement officers, authorising officers and Heads of Service.

The Council's processes and practitioners were inspected by the OSC during August 2015 and were found to be satisfactory. The OSC commended the Council's procedure which ensures that its authorising officers are not based within the service applying for

authorisation. The OSC recommended that minor changes were made to the Council's Policy and these have now been made.

The Council will also extend corporate oversight over the use made of surveillance that is not regulated by RIPA by establishing a process for authorisation of Non-RIPA surveillance.

A summary of the Council's use of RIPA during the year is summarised in **Appendix I**.

6.3 Office of Surveillance Camera Commissioner

The Office of Surveillance Camera Commissioner (OSCC) oversees compliance with the surveillance camera code of practice. The office of the commissioner was created under the Protection of Freedoms Act 2012 to further regulate CCTV. The Council completed the OSCC's self-assessment toolkit in December 2015; an action plan will be implemented. The Council has begun a process of assisting its schools to gain assurance concerning compliance with the Surveillance Camera Code of Practice.

7. Conclusions

The SIRO considers that there is significant documented evidence to demonstrate that:

- the Council's arrangements for IG and data protection compliance are reasonably effective;
- much progress has been made (from a low base) to implement the recommendations of the ICO's audit work, and enforcement activity;
- the measures required are not yet fully implemented, and where they are implemented, they are not yet sufficiently matured to yet justify an enhanced level of assurance;
- to move to a higher level of assurance will require implementation and successful testing of the steps described in this report;
- the Council's overall (there is variance between services) data protection compliance remains a medium risk to the Council.

Appendix A

Wales Accord on the Sharing of Personal Information (WASPI) **Information Sharing Protocols in development:**
Single Point of Access (SPoA) to Community Services, Anglesey
Flying Start (Anglesey)
Team Around the Family
Trading Standards *Buy with Confidence* North Wales Region
Anglesey and Gwynedd Integrated Family Support Service

Appendix B

Data security incidents
Level 0 – Level 1 Incidents: 6
Level 2 incidents: 0
Incidents reported to the ICO: 0

Appendix C

Freedom of Information Act Complaints
4 Complaints to the ICO were made in this period.
1 required a response to be sent to the complainant;
2 decisions upheld the original decision; 1 decision notice is awaited.

Appendix D

Freedom of Information Act complaints and Internal reviews
17 complaints and requests for Internal Reviews received

Appendix E

Data Protection Act Complaints to the Council
1 DPA complaint was made, investigated and not upheld.

Appendix F

Subject Access Requests and compliance
28 SARs were received.
65% were responded to within the 40 day timescale.

Appendix G

ICO Enforcement Notice Action	Status	RAG status: Green = completed; Amber= on track; Red = overdue
1. Data protection KPI's and measures are monitored and acted upon (including the number and nature of information security incidents)	Data protection KPIs are now in place and reported.	
2. There is a mandatory data protection training programme for all staff (including new starters) and refresher training on an annual basis	There is a mandatory data protection training programme in place and the Council is looking to develop an e-learning package.	
3. Completion of any such training is monitored and properly documented	Completion of training is now monitored and properly documented.	
4. Policies (including the Records Management Policy) are being read, understood and complied with by all staff	The Council has undertaken a manual sign-up process to provide assurance. A policy acceptance system is currently being implemented and developed.	
5. Information is backed up to an external server on a daily basis	This is now achieved.	
6. Back-ups are tested periodically to ensure that they have not degraded and that information is recoverable	This is due to be completed in August 2016.	
7. Physical access rights are revoked promptly when staff leave and periodically reviewed to ensure that appropriate controls are in place.	The issue of access rights is being considered as part of a business re-engineering of the starters and leavers process which is being undertaken to provide assurance in this area.	
8. The lack of adequate storage solutions for manual records is addressed	This is now addressed, with the Council's Corporate Information Governance Board retaining oversight of departmental record action plans.	
9. Consistent and regular monitoring is undertaken to enforce the clear desk policy	This is now in place and monitored by a performance indicator.	

Appendix H

Summary of CIGB I.G. Action-Plan	
Version control	Version control to be introduced on all data protection policies.
Policy amendment	Consult the ICO PIA Code of Practice when amending policy
	Amend reference to IGB to CIGB
	Include review information in RM policy.
	Review Privacy Notice Policy to establish whether the fixed templates are suitable.
	Data Classification Policy to be amended in order to set out how protectively marked information should be stored.
	ICT Security Policy to include starters & movers process.
	Correct incorrect references in ICT Policy
	Information Security Policy to include security of manual records.
	Seek assurance about retrieval of hardware as part of the leavers / movers process.
	Include review information in RM policy.
	Review Privacy Notice Policy to establish whether the fixed templates are suitable.
	Data Classification Policy to set out how protectively marked information should be stored.
	Information Security Policy to include security of manual records.
	Review of Fair Processing Notices to ensure adequacy.
Policy compliance	Assurance about suspension of access to accounts
	PIAs as part of Project Management methodology. Smarter Working Programme Board to report to CIGB on a yearly basis
Identification of assets and risks	Develop the Information Asset Register
	Develop a corporate data security incident log.

	Develop an Information Sharing Protocol (ISP) register.
	PIA Process to include sign-off and training
Effective management of offsite records storage.	CIGB to issue a directive to IAOs to seek their assurance that offsite areas are managed in accordance with relevant policies.

Appendix I

Regulation of Investigatory Powers Act	
Number of Directed Surveillance authorisations granted:	0
Number of Directed Surveillance authorisations in force:	0
Number of authorisations presented to a magistrate:	1
Number of authorisations rejected by a magistrate:	0
Number of Property Interference authorisations granted:	0
Number of Intrusive Surveillance authorisations granted:	0
Number of CHIS authorisations extant on 1 April 2015:	0
Number of CHIS authorisations granted:	1
Number of CHIS authorisations cancelled:	1
Number of CHIS authorisations extant at 31 March 2016:	0