CYNGOR SIR YNYS MON / ISLE OF ANGLESEY COUNTY COUNCIL	
MEETING:	**AUDIT & GOVERNANCE COMMITTEE**
DATE:	**21 September 2017**
TITLE OF REPORT:	**INFORMATION GOVERNANCE – SENIOR INFORMATION RISK OWNER'S ANNUAL REPORT FOR 1ST APRIL 2016 – 31ST MARCH 2017**
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 2016 – 31 March 2017 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 2016-2017; 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. This report follows the format of the previous Annual 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 currently 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 (Data Protection Officer)**
- **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 **Wales Accord on the Sharing of Personal Information** (WASPI) 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 The General Data Protection Regulation.

Looking to the future, data protection is entering upon a period of unprecedented change; in May 2018, the General Data Protection Regulation (GDPR) replaces the Directive 95/46/EC, which has been the basis of European data protection since 1995. The General Data Protection Regulation (GDPR) will replace much of the existing data protection legislation in May 2018.

The GDPR introduces more stringent and prescriptive compliance challenges, underpinned by a more punitive regulatory environment. The GDPR will punish non-compliance, resulting in serious regulatory penalties of up to the equivalent of €20 million euros, possible litigation and serious reputational harm.

However, rather than an enhanced level of potential fines, the real risk to the Council is that the scope of activities for which the Council may be fined is broadened.

The Council must continue to establish a culture of monitoring and accountability regarding its processing of personal data. GDPR states that not only shall the Council be responsible for compliance, it must be able to demonstrate compliance with the data protection principles.

Accountability is an important element in GDPR and central to compliance with it. The enhanced requirements of GDPR represents a fundamental challenge to the Council, as GDPR requires a shift towards a granular monitoring and documenting of evidence. Work to implement the GDPR is tabled to begin in September 2017, (following publication of the White Paper) followed by an audit of GDPR readiness by Internal Audit and reporting to the Senior Leadership Team.

Clearly, non-compliance with GDPR is likely to be the primary information risk for the Council.

5.2 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 CIGB has developed the first version of the Council's Information Asset Register.

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. Whilst development work to identify the main risks associated with each of the Council's business critical systems and assets was tabled for further development this year, the

forthcoming GDPR requires that work on other aspects of the IAR be prioritised. The Information Commissioner advises that the IAR should be developed as the key assurance record of processing activities, in readiness for the implementation of the GDPR. This work is being undertaken regionally through the North Wales Information Governance Group in order to ensure a consistent approach to the accountability requirements of GDPR and to share capacity and expertise in the most effective way possible.

5.3 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 Policy Portal. The policies are reviewed and updated by the CIGB. This work is timetabled and will always be subject to an ongoing programme of 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 (see 5.4 below). This ensures that employees are clear what the Council's expectations are regarding information security.

It is anticipated that the implementation of the GDPR in 2018 will require the review of all Council IG policies, particularly as the UK implements domestic legislation (post September 2017). It is likely that the Council will need to develop and adopt new policies to respond to the broader extent of the GDPR, particularly in the area of data subject rights.

5.4 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 Information Commissioner highlighted this element in the 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.

The Council implemented its policy management system, *Policy Portal*, which has served as a library of policies since November 2016. The policy acceptance function was introduced in April 2017 (outside the period of this report). *Policy Portal* will provide the SIRO with assurance that key IG policies are being read, understood and formally accepted by individual members of staff.

5.5 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. A PIA is often the most effective way to demonstrate how personal data processing complies with the law.

Conducting a PIA is not currently a legal requirement of the Data Protection Act 1998, nonetheless it will become compulsory in May 2018 as part of the General Data Protection Regulation.

It is necessary for PIAs to be undertaken when a project is being considered, or some new variation of an existing activity will result in using personal data in a different way. The GDPR requires that any new processing that involves a high level of risk to people's personal data will require an assessment of this impact prior to starting the work. In matters of severe risk to privacy, the Information Commissioner will require that she is alerted to the proposed processing before it commences.

The SIRO considers that compliance with the GDPR will require the Council to embed the principles of *Privacy by Design*, meaning that privacy implications of new or changed processes must be considered. This will require establishing a process for identifying when a PIA is required, and also suitable methodologies for undertaking this work. Work on drafting a new process commenced during this period; however, the European Data Protection group did not publish its guidance on data protection impact assessments until after the period of this report.

During the period of this report **two** PIA's were completed. In the midst of a transformation agenda we are sceptical about the level of compliance in this area. Its significance to GDPR is likely to make it a feature of the post White Paper review by Internal Audit.

5.6 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.

In addition, appropriate training is given to Staff with IG roles.

5.7 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. Assured ISPs are published on the Wales Accord on Sharing of Personal Information Website.

The Council also participates in the Quality Assurance process of WASPI ISPs through the North Wales Information Governance Group.

5.8 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).

It is not yet clear whether major revision of the Council's methodology will be required in order to comply with the GDPR.

The number of incidents recorded by the Council is provided in **Appendix A.** It is evident that the proportion of Level 0 – Level 1 incidents has risen sharply (from 6 in the previous report). A significant proportion of the incidents have involved information being sent by email.

The SIRO considers that the increase in **< Level 1** breaches being reported is due to an encouraging increased awareness of the need to report data security incidents, rather than a worsening of data security.

5.9 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.

An audit of GDPR readiness will be undertaken by Internal Audit during October – December 2017.

5.10 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 B**. (16/17). In addition, the Council also holds, at the request of complainants, Internal Reviews of its responses under FOIA; this information is also provided at **Appendix B**.

The Council also investigates complaints made to it about data protection matters; further information is provided in **Appendix C**. (16/17)

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 (SARS) are often complex and resource intensive. Information about the number of Subject Access Requests and the Council's compliance is provided in **Appendix D** (16/17). The majority of SARS are received by Social Services and are complex to process.

The CIGB will design new performance indicators (they are already in draft) in readiness for the implementation of GDPR in May 2018.

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'.

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 the subject of an 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 contained 41 actions which were required to implement the nine recommendations. The Enforcement Notice Action Plan is now completed and a summary of the nine headings of the Enforcement Notice Action Plan is presented in **Appendix E.** A closure report to the Council's Senior Leadership Team is tabled for September 2017.

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 waywhich 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.

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 been made.

During the past year, the Council has also developed a draft process for authorisation of Non-RIPA surveillance. However, the research undertaken demonstrates that there are no grounds for concern that extensive use of surveillance that is not regulated by RIPA is undertaken at the Council.

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

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. The Council has begun a process of assisting its schools to gain assurance concerning compliance with the Surveillance Camera Code of Practice and developing suitable policies.

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 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.
- any failure to implement and comply with the GDPR will be a major risk for the Council.

Appendix A

The number of incidents recorded by the Council during the period of the report.

Data security incidents (16/17): 34 incidents	
Level 0 – Level 1 Incidents: 33	*Breakdown:* *Disclosed in Error* = 21 (13 involving autocomplete) *Technical / Procedural failure* = 2 (Using incorrect e-mail address / Printer) *Lost data/ hardware* = 2 (form lost / file left behind) *Lost in transit* = 2 (Files requested from Care Home never arrived / Documents lost) *Non Secure disposal* = misplaced document *Other* = 5
Level 2 incidents: 1	
Incidents reported to the ICO: 1	

Appendix B

The number of Freedom of Information Act Internal Reviews undertaken and the number of complaints to the ICO processed by the Council during the period.

Freedom of Information Act requests for Internal Review (16/17)
12 requests for Internal Review received by the Council.

Freedom of Information Act Appeals to the ICO (2016 / 2017)
6 appeals were lodged with the ICO in this period.
6 appeals upheld the original decision of the Council.

Note:

If requestors are unhappy with the original response they can request an Internal Review (appeal) which must be undertaken by the Council's Corporate Information Governance Manager.

If the original response is upheld at Internal Review then they may take the matter to the ICO who will assess whether or not to investigate.

Appendix C

Information about the number of data protection complaints made to the Council by individuals about its processing of their personal information.

Data Protection Act Complaints to the Council (16/17)
2 DPA complaints were made and investigated: 1 was not upheld. 1 was upheld (complainant advised to refer their complaint to the ICO).

Appendix D

Information about the number of data protection Subject Access Requests and the Council's compliance within the period.

Subject Access Requests and compliance (16/17)
29 SARs were received.
45% responses within the 40 day deadline.

Appendix E

A summary of the Council's compliance with the nine headings of the ICO Enforcement Notice Action Plan.

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 developing 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 undertook a manual sign-up process to provide assurance. A policy acceptance system is now implemented and monitored.	
5. Information is backed up to an external server on a daily basis	This is now completed.	
6. Back-ups are tested periodically to ensure that they have not degraded and that information is recoverable	This is now completed.	
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. (Northgate implementation)	
8. The lack of adequate storage solutions for manual records is addressed	Issues at both sites resolved.	
9. Consistent and regular monitoring is undertaken to enforce the clear desk policy	This was monitored by a performance indicator but now through Policy Portal/IAOs.	

Appendix F

A summary of the Council's use of the Regulation of Investigatory Powers Act 2000 during the period.

Regulation of Investigatory Powers Act		
i.	How many Directed Surveillance authorisations were granted?	**Nil**
ii.	How many Directed Surveillance authorisations remain extant?	**Nil**
iii.	How many authorisations were presented to a magistrate?	**Nil**
iv.	How many authorisations were rejected by a magistrate?	**Nil**
v.	How many Property Interference authorisations were granted?	**Nil**
vi.	How many Intrusive Surveillance authorisations were granted?	**Nil**
vii.	How many CHIS authorisations were extant on 1 April 2016?	**Nil**
viii.	How many new CHIS authorisations have been granted?	**Nil**
ix.	How many CHIS authorisations were cancelled?	**Nil**
x.	How many CHIS authorisations remain extant at 31 March 2017?	**Nil**
xi.	How many authorisations using s49 Encryption powers were granted?	**Nil**
xii.	How many times were urgency provisions used, including the type of authorisation?	**Nil**