Economy, Residents and Communities Scrutiny Committee

Scrutiny Observations to Cabinet on: 20th December 2022

The Economy, Residents and Communities Scrutiny Committee undertook a virtual scrutiny of the following documents:

- Annual Information Governance Report 2021-2022

Scrutiny made the following observations:

Section 3:

Clarification: • Consideration be given to elements of the plan being grouped in terms of priority / significance to clarify that the most important actions have been completed or the inclusion of a statement such as "Of those not complete, none are considered to be creating a risk and a plan is in place for all to be treated taking account of the urgency of each one". • The standard to which elements in the plan are completed and what this means for data security. • Why the timescale for the 32 elements had been revised and when would they be completed. • Why 2 elements were unlikely to be completed in the timescale, and 3 were out of the timescale. • The total number of elements comes to 60 rather than 61.
Response Elements of the Information Assurance and Governance plan are grouped in relation to their activity and outcomes, such as Training, Governance, Monitoring, Information Security etc. All elements if not completed contain an element of risk, but not just relation to information security but also into compliance, and risk management. However, going forward the Corporate Information Governance Group have agreed that elements of the 21-23 plan can be simply risk rated, indicating the level of risk to the organisation if not completed, which can then be included in next year's annual Information Governance report. Timescales have been changed due to limitations in respect of resources, dependencies on other elements, and other work activities taking priority. Authority to change timescales are sought from the Corporate Information Governance Group. At the time of developing the annual report then one elements of the plan had been newly added and was awaiting timescales to be agreed by the Corporate Information Governance Group, which was due to have taken place in March, but which was cancelled.
Questions:

- Whether the number of reported incidents has increased due to better reporting or familiarisation with the policy to report data breaches.
- To complete the plan to timescale should the CIOG meet more often than every 6 weeks.
- Why were elements of the plan not completed.

Response
The report indicates that it is not possible to identify precisely why the numbers of incidents being reported have increased. Potentially due to better understanding of policy, what constitutes an incident, and realisation that the Information Compliance team are available to assist when such incidents occur.

The Corporate Information Operational Governance Group in most cases doesn't complete elements of the plan, and as such meeting more frequently would result in less available time for those staff tasked with completing elements of Information Management Assurance Governance plan.

Elements of the plan have not been completed due to resource limitations, dependencies on other elements, and other work activities taking priority.

Comment:
- Disappointed that as at 31-03-22 only 23 of 61 elements completed (38%)
- Reasonable progress against the plan and further time will see a further 52% achieved.
- Almost impossible to achieve 100% completion.

Response
Disappointment at non completion of some elements noted.

Section 4:

Clarification:
- The numbers of staff required to take annual training and the process for renewing training to ensure compliance.

Response
All staff will be required to refresh their Cyber Security and GDPR training annually in line with their own training anniversary. The report indicates that on 31st March 2022 there were 3254 staff who had a requirement to undertake the training and of those 2374 had completed their training and weren't overdue on the refreshing of their training.
When training is due to be refreshed then Trent will email the user and their line manager a month before, and the user completes the Cyber Security and GDPR eLearning course. This course is updated annually.

Questions:
- What actions are being taken with those areas of the organisation with high levels of noncompliance.
- Is there an understanding why staff and Members were not completing their training and what was being done to address this.
- Why is staff compliance rate decreasing.

Response

Managers are required to ensure that their staff undertake and refresh their training as required. Escalation processes are being considered by Workforce and Organisational Development for noncompliance for all mandatory training.
It is not known why training is not being completed or refreshed. Anecdotally reasons given, as lack of time, not using completers for work, not being aware that refresh is due etc. Workbooks are available for staff who are unable to access the eLearning electronically, reminders are issued from Trent, the annual appraisal asks if mandatory training is completed. Training compliance is discussed at Senior Leadership Team.

Comment:

- Training needs to target the services where breaches are most prevalent.

Response

A personal data breach can occur in any service, hence training being undertaken by all staff, when breaches occur then records are checked to ensure that staff involved have completed their training. Where they haven't don't so then this is escalated.

Section 5:

Clarification:

- Understanding of incidents reported and determination of data breaches and the reporting process.
- Understanding of why we are having data breaches and are they significant or minor.

Response

A personal data breach is defined with data protection legislation, however some incidents reported do not meet the definition, but reporting and the further consideration of the incident enables the Council to have a wider vision of vulnerabilities and risks, and potentially enables actions to prevent a personal data breach.
When an incident is first reported to the Information Compliance team then consideration is given as to whether a personal data breach has occurred. If so then further consideration and assessment is undertaken as to whether the thresholds of reporting to the Information Commissioner's Office and data subject(s) has been reached. Whether the threshold of reporting to the Information Commissioner's Office has been reached will be determined by the Council's Data Protection Officer, and the subsequent report issued, within 72 hours as directed by data protection legislation. If the threshold of reporting to the data subject(s) has been reached also then the service will develop and issue the appropriate notification with assistance from the Information Compliance team.
The majority of personal data breaches are due to human error, for example choosing the wrong email address, or the wrong attachment, but some are due to a failure to follow policies and processes. Anecdotally staff indicate they made errors when rushed or trying to multitask.
All personal data breaches have the potential to be significant to the organisation and the data subject(s). For example, a misdirected email can have very little impact or have a very serious impact, dependent upon numerous factors, such as the recipient, the personal data items involved etc. The report indicates that 11 personal data breaches out of 149 were assessed as being so serious that they required reporting the to the Information Commissioner's Office.

Questions:

- Is there any correlation between the data breaches and those who did not undertake the training.
- Is there a pattern of incidents.
- What action is being taken to address incidents and reduce the breaches.
- Why is the reason for incidents not known.
- Why has the number of incidents increased.

Response

No correlation between personal data breaches and noncompliance with Cyber Security and GDPR training has been identified. However, when reporting to the Information Commissioner's Office then the Council is specifically asked is staff have received training within the last 2 years. If not known at the time, then the response is made clear within investigation outcome reports which are subsequently issued.

Appendix 2 of the report indicates that the majority of these incidents relate to unauthorised disclosure of information, many of these are the result of misdirected emails, due to the officer selecting the wrong email address, or attaching the wrong document to the email they are sending. Where trends are identified then these are raised directly with the Head of Service, these could relate to a set of actions occurring, or failing to be followed, or be in respect of a member of staff.

With human error being the factor in many being, it is not possible to fully prevent these errors, however Information Governance training and awareness is raised regularly as a remainder to take care with information. The development of documented processes, and process map can also provide staff with the correct instructions to follow. The Information Compliance team will offer to attend team meetings to discuss a specific incident or incidents in general. Training has been provided for some services who carry out redaction and disclosure of information.

It is not always possible to know why a mistake is made, though staff some time indicate that they are rushed. Where a reason for the incident(s) occurring has been identified then actions can be taken in an attempt to prevent a reoccurrence. Such as turning off autocomplete in Outlook, or clearing autocomplete history, adding Powys Teaching Health staff to the Outlook address book, including officers' roles into the Outlook addresses book, undertaking testing of the consequences of IT solution implementation on the personal data affected etc.

The increase of incidents is potentially due to better understanding of Council policy on reporting, or understanding what constitutes an incident, and realisation that the Information Compliance team are available to assist when such incidents occur.

Comment:

- The rise in breaches is an issue as we have received comments and recommendations from the Information Commissioner's Office.

Noted

Section 6:

Clarification:

- How many FOI requests were rejected and how much resource is taken up responding to requests.

Response

No information request is rejected, every request received must have a formal response issued, even if the request for information is being refused. Requests can only be refused based upon an exemption provided within the differing legislation, of Freedom of Information 2000, Environmental Information Regulation 2004 and UK General Data Protection Regulations.
An exercise was undertaken in 2019 in an attempt to establish resources and costs. In one month, 528-man hours were spent dealing with 115 Freedom of Information and Environmental Information Regulations requests. These averaged out at 4.5 hours each. Using the same financial amount as given under the Appropriate Fees and Limits Regulations to calculate costs, then each request cost £114.75. Therefore with 1020 Freedom of Information and Environmental Information Regulations requests received on 21-22 this would equate to 4,590-man hours and costing £114,750.

Questions:

- Has any research been done to find out how to reduce the number of requests received and if all information was readily available in the public area would this reduce requests.
- Is the delay in responding to requests due to officer workload or another factor.
- What is the impact of noncompliance – increased inspection or cost of officer time, fines or poor reputation or lack of confidence in the Council.
- What action is taken if a service is late responding.
- Why is there a low compliance rate for SARs.
- What can be done to mitigate a 11% increase in SARs.

Response

Where information is regularly sought then the Service Area are asked to publish and maintain the information on Council web pages. Requests very often follow decisions of the Council, and as such the publication of information informing the decision can be beneficial. However even if the information is published this doesn't necessarily prevent the requests being made, as the public don't always check the web pages, and so a refusal decision with the relevant exemption and links to the information still have to be issued.
Delays can be caused by officer workload, competing priorities, difficulties gathering the information. In terms of Subject Access Requests this is generally due to Information Compliance Officer workload and volume of information to be examined to determine if the data subject is entitled to the information.
The pictures at appendix 1 indicate the amount of information to be examined within a Subject Access Request. These pictures were taken when the work was undertaken manually.
Consequences of non-compliance with Freedom of Information and Environmental Information Regulations can result in public reprimand from the Information Commissioner, decision notices requiring certain actions to be carried out.
Whereas the consequences of noncompliance with Subject Access Request could result in fines, as a maximum penalty. Recently the Information Commissioner has publicly criticised a number of organisations including Government departments for their failures in responding to Subject Access Requests.
If a service area is late in providing information to the Information Compliance team, then an escalation process is followed in informing the Head of Service and then the Director.
Data protection legislation provides a right of access to personal data being processed by an organisation, and when the GDPR was implemented in 2018 a great deal of publicity surrounded this right of access, even though it existed in previous legislation. The service areas are able to provide individuals with copies of documents taking into account any information of third parties etc. However, in many

cases the public are advised that a SAR is the appropriate route to take. In some local authorities Subject Access Requests for Social Services information are undertaken by the services directly.
Comment: • Reasonable compliance across most request types.
Noted

Section 11:

Clarification: • Details of who is the Senior Information Risk Owner and where they sit in the staffing hierarchy. • Why is electronic information stored in a hard copy. • Could the FTE for staff be provided as difficult to assess whether staff are full or part time.
Response The Senior Information Risk Owner is the Head of Legal (Monitoring Officer) Section 11 refers to the work of the Information Management team, who store and manage all the Council's inactive hard copy records, these are generally those records predating electronic record keeping. Where requests were made for hard copy records by the services from storage, then the smaller files were scanned and sent to the requestors electronically, rather than sending a hard copy file to staff who are working from home. All staff referred to in Section 7 are all fulltime.
Questions: • What penalties can be imposed on the Council if training requirements were not met. • Is there a role for the Governance and Audit Committee in oversight of the governance of Information Management.
Response Strictly speaking failure to comply with the enforcement notice issued in 2012, could be considered as contempt of court which is an imprisonable offence. However, in moving to a 12-month refresh period the Council now exceeds the timescales referred to in the notice, but the notice still calls of all staff to be trained. The Corporate Information Governance Group oversees activities feeding into the Council's Information Governance framework within Powys County Council, which in turn feeds into the Corporate Governance of the organisation. Cabinet oversees this work through the Annual Information Governance report, and whilst there is no statutory requirement for this report to be developed it is considered good practice and utilised by several local authorities in Wales.

Section 12:

Clarification: • An index of abbreviations / acronyms to assist the reader's understanding.
Response See Appendix 2 -those highlighted indicate those missed from the report
Questions: • Have the main risks been identified and are measures in place to minimise those risks.

• Is there a need for more staff and resources for training.
Response Non-Compliance with data protection legislation remains a high-level risk on the Council's Risk Register and many elements of the Information, Management, Assurance, and Governance plan feed into the controls to mitigate that risk. Whilst each element of the plan isn't risk assessed priority is given to those elements which improve those controls or result in a compliance with other information obligations.
Comment: • Appreciate that in relation to organisational non-compliance 69% in April 2021 and 59% in March 2022 relates to Highways, Transport and recycling and Housing and Community Development where employees do not have laptops and further work is required. • Progress is clearly being made.
Response Highways, Transport and Recycling utilise "toolbox" talks to deliver training. With the changes in directorates and services then the Cleaning service is noted as that affecting the Housing and Community Development noncompliance. The new Interim Head of Service has been made aware of the need to improve compliance rates.

Any Other Questions / comments:

•
• The numbers of breaches of compliance in Adults and Children's Services is of concern.
• Noted to be raised at Corporate Information Governance Group

Scrutiny's Recommendation to Cabinet	Accept (plus Action and timescale)	Partially Accept (plus Rationale and Action and timescale)	Reject (plus Rationale)
1 That the Cabinet be requested to provide the scrutiny committee with: (i) a clarification of the points raised; and (ii) a response to questions and comments.	Responses for clarification, questions and comments included above.		

In accordance with Rule 7.27.2 the Cabinet is asked to provide a written response to the scrutiny report, including an action plan where appropriate, as soon as possible or at the latest within 2 months of the date of the Cabinet meeting i.e. by 20th February 2023

Membership of the Economy, Residents and Communities Scrutiny Committee on 2022-23:
County Councillors:

A Davies, D Bebb, A Cartwright, T Colbert, B Davies, I Harrison, Adrian Jones, Arwel Jones, K Lewis, G Mitchell, J Brignell-Thorp, C Walsh, S Williams.

Appendix 1

Appendix 2

Abbreviations

Corporate Information Governance Group	CIGG
Corporate Information Operational Group Governance	CIOG
Data Protection Act	DPA
Data Protection Officer	DPO
Department of Work and Pensions	DWP
Environmental Information Regulations	EIR
Executive Management Team	EMT
Freedom of Information Act	FOI
General Data Protection Regulations	GDPR
Information Asset Owners	IAO
Information Assurance for Small to Medium-sized Enterprises	IASME
Information Commissioner's Office	ICO
Information Governance	IG
Information, Management, Assurance and Governance	IMAG
National Health Service	NHS
Public Services Network	PSN
Regulation of Investigatory Powers Act	RIPA
Secure Access Service Edge	SASE
Senior Information Risk Owner	SIRO
Subject Access Request	SAR
Term of Reference	ToR