Fraud and Data Team Update

Executive Portfolio Holder:	*Peter Seib, Finance and Legal Services*
Director:	*Ian Clarke - Support Services Director*
Service Manager:	*Lynda Creek - Fraud and Data Manager – Fraud and Data Service*
Lead Officer:	*Lynda Creek - Fraud and Data Manager – Fraud and Data Service*
	Zoe Rodgers – Fraud and Data Officer - Fraud and Data Service
Contact Details:	*lynda.creek@southsomerset.gov.uk or 01935 462204*
	zoe.rodgers@southsomerset.gov.uk or 01935 462512

Purpose of the Report

1. *The report is provided in response to a request from members for an update on the Summary of Significant Risks, provided by the South West Audit Partnership (SWAP), at the last Audit Committee Meeting. Although the Fraud and Data Team were only mentioned in some of the recommendations (all of which have been met) an update is provided on the others so as to provide a fuller picture for members;*

Public Interest

2. *The Summary of Significant Risks set out some key concerns that the SWAP auditor had identified and the recommendations they has made to deal with these risks. In essence, the audit was about whether, when a service (or part of it), is undertaken by someone other than SSDC staff, the legal requirements on how the personal data of customers is handled have been met e.g. would the contractor have sufficient security measures in place to protect the data from unlawful disclosure. loss, theft, unauthorised amendment or destruction etc. This issue is one which is often overlooked and an audit was commissioned by the Fraud and Data Team to assess the extent of the issue. The 'Summary of Significant Risks is the response to the matters identified in the audit.*

Recommendations

3. That the Audit Committee note the contents of the report

Background

4. Under the Data Protection Act 1998 (DPA) where a Data Processor (basically a third party such as a contractor) processes personal data about individuals on behalf of the Council certain legal requirements must be in place before any processing starts. These include a written contract containing certain mandatory conditions; checks on the technical and organisational security measures in place to protect the personal data (including staff training) and on-going monitoring of these measures to ensure the contractor complies with them and reports and breaches

5. It had been identified by the Fraud and Data Team that these requirements are very often not followed and where such breaches are identified it is much harder to rectify once the contract has started and personal data is being processed by the third party. An audit was commissioned to examine the extent of the issue and the recommendation in the Summary, broadly represent the findings of the audit

Report Detail

6. The Summary of Significant Risks is reproduced as an Appendix A for reference purposes and the response to each point is set out in a Appendix B as there was insufficient room to do so on the Summary form itself

Financial Implications

7. Breaches of the Data Protection Act 1998 can result in financial penalties of up to £0.5m as well as other sanctions. Under the General Data Protection Regulation, which comes into force next May 2018, the scope for such penalties rises to around £9m so this is a very important issue.

Council Plan Implications

8. There is no specific reference to data protection, privacy or information assets in the Council plan but it is a legal requirement and implicit in providing high quality services to the public.

Carbon Emissions and Climate Change Implications

9. N/A

Equality and Diversity Implications

10. Although there may be equality issues around the selection of 3rd parties to undertake work for the Council, this audit was focussed on compliance with legal requirements so an EIA is not required.

Privacy Impact Assessment

11. N/A

Background Papers

12. N/A