Appendix A

Schedule of potential significant risks identified from Internal Audit work in the period Quarter 1 and Quarter 2

Ref	No	Name of Audit	Weaknesses Found	Risk Identified	Recommendation Action	Managers Agreed Action	Agreed Date of Action	Manager's Update (Date)
35702		Data Protection	For individuals supporting the Authority, either by secondment or as private contractors paid through the Authority's payroll system, there was insufficient assurance that they have been fully trained with regard to data protection requirements. There is also some uncertainty as to their status, i.e. whether they are	If they are data processors rather than employees then the authority is in breach of the DPA. There is an increased risk of fines and reputational damage if these individuals are responsible for further data breaches.	I recommend that the HR Manager/Housing and Welfare Manager as appropriate should confirm the status of these officers (within the context of Data Protection legislation). If it is determined that individuals are employed on a secondment basis or are considered employees, confirmation should be sought that data protection induction and	HR Manager - The Interim Assistant Director for Transformation has been provided with a copy of the induction programme which includes guidance on Data Protection provided to all staff on induction. H&W Manager – Confirmation to be obtained regarding Homefinder Scheme Co-ordinator status and Data Protection induction.	31st May 2017	

			employees or contractors.		training has been carried out. If the individuals are considered private contractors, a written contract covering data protection issues should be used.			
35703		Data Protection	Where contracts are in place, these contracts often lacked sufficient detail re the data processing requirements and service managers should have sought input from the Fraud and Data Team if they were unclear what the DPA required.	The Authority may be unable to demonstrate it has taken reasonable steps to ensure the safety of personal data handled by Data Processors, resulting in larger fines and greater reputational damage.	I recommend that the Procurement and Risk Manager should issue a reminder to all Service Managers, stating that where contracts are to be extended beyond their natural term, advice is taken from the Procurement and Risk Manager on the legality of the extension (which may otherwise be unlawful), and written confirmation and	Agreed. Reminder to be issued.	31st July 2017	

					authority for this extension should, as a point of good practice, be drawn up and held with the contract documentation in the Deed Room.			
35704		Data Protection	Where contracts are in place, these contracts often lacked sufficient detail re the data processing requirements and service managers should have sought input from the Fraud and Data Team if they were unclear what the DPA required.	The Authority may be unable to demonstrate it has taken reasonable steps to ensure the safety of personal data handled by Data Processors, resulting in larger fines and greater reputational damage.	I recommend that the Fraud and Data Manager issues a reminder to all Contract Managers that where contracts are renewed or it is agreed to roll them forward, that data protection issues are covered.	Happy to do this.	28th April 2017	
35707		Data Protection	The central repository for contracts, maintained by the legal team,	Contracts may be hard to or impossible to locate as responsible officers	I recommend that the Procurement and Risk Manager should arrange for A copy of all	Agreed. Service areas to be made aware.	31st July 2017	

			is often not used by service areas. We found that in the majority of instances service managers retain the only copy of contracts in their services' area.	change posts or leave. In the event of a major incident such as a fire/flood, paper based contracts may be permanently lost. The Authority may be unable to enforce contractual obligations including those relating to data protection or demonstrate that reasonable steps were taken to ensure the data protection requirements were met.	significant contracts, including low value contracts where there are significant risks in terms of DPA compliance, to be lodged with the legal team for retention within the central repository. The Procurement and Risk Manager should ensure that all service areas are aware of this requirement.			
35708		Data Protection	Where contracts are in place, these contracts often lacked sufficient detail re the data processing requirements and service managers should have	The Authority may be unable to demonstrate it has taken reasonable steps to ensure the safety of personal data handled by Data Processors, resulting in larger fines and greater reputational	The Fraud and Data Manager should issue a reminder to all service managers that they should liaise with her when drafting any contracts with Data Processors, to ensure that all	Happy to do this again (have already made aware in past).	31st May 2017	

			sought input from the Fraud and Data Team if they were unclear what the DPA required.	damage.	relevant clauses are included.			
35709		Data Protection	A contract could not be located for the Out of Hours Service.	This is a breach of the Data Protection Act and if the ICO became aware it could result in heavier penalties being imposed on the Authority.	I recommend that the Civil Contingencies Manager should put a formal agreement in place between the Authority and the Deane Helpline Service, covering all necessary data protection responsibilities and obligations including liaison with the Fraud and Data Team as necessary.	Agreed.	31st October 2017	

Summary of key points related to 'Partial Assurance' reviews

Audit Title	Significant Audit Findings	Key Actions Agreed by Service	Dates of Agreed Implementation	Date of programmed follow up
Data Protection	A partial Assurance rating was given for the following reasons: • Only a small number (3 out of 12) of contracts/agreements from our sample were catalogued and held in the central repository (consisting of a fire proof room) by the legal team. There is a risk that this could lead to the permanent loss of contract documents, which in turn could lead to difficulties in dispute resolution with regard to data protection issues with data processors. • Contracts were also not in place for all data processors which is a direct breach of the Data Protection Act. • Service areas conducting procurement exercises where data processors are to be used are not ensuring the requirements of the DPA are met. They are not, generally, seeking advice from the Fraud and Data Team at an early stage which reduces the level of expertise used when developing such arrangements and increases the risk of a breach. • Transmission of data between the Authority and data processors was not always carried out securely and although not generally of a sensitive	As detailed in the above table.	As above	TBC

Audit Title	Significant Audit Findings	Key Actions Agreed by Service	Dates of Agreed Implementation	Date of programmed follow up
	nature, a breach could result in financial penalties being incurred. • The Authority utilise a number of individuals in roles that have access to personal data who are not direct employees but are also not treated as data processors and so have not been subject to a formal contract containing the mandatory conditions nor have they met the other DPA requirements e.g. concerning security measures.			