ERP B - Data Protection Action Plan

Observation	Risk	Risk Rating	Recommendation	Agreed Yes/No	Management Response	Target
1. There is no formal Information Governance Management Framework to manage Data Protection and Information Security.	Without a recognised framework, There is a risk that Data Protection (DP) and Information Security (IS) issues could be overlooked, leading to organisational systematic errors.	**H**	An Information Governance (IG) Framework is put in place to manage Data Protection and Information Security as a central part of the business. All service areas should play a key role within that framework which feeds into the Councils Corporate Management Team. Key components under this Framework will consist of • Information Governance Management • Confidentiality and Data Protection Assurance • Information Security Assurance (Support and Infrastructure, both physical and electronic) • Data Sharing (internal and External) Use Assurance • Corporate Information Assurance	**Yes**	The council considers that this endeavour should be adopted into the standing agenda of Senior Management Group and the Corporate Management Team. By directly integrating IG into the roles of the existing Senior Management Group, the council believes this will close the gap between strategic/corporate management and operational management, creating a more engaged approach and strengthening the service level understanding and application of DP Principles The following steps are under consideration: Data Protection Compliance Governance Framework DP and IG to become a standing item on CMT Agenda DP and IG to become standing item on SMG Agenda DP and IG to become a standing item on IT Steering Group Agenda **GREEN - COMPLETED**	**31/12/12**

ERP B - Data Protection Action Plan

Observation	Risk	Risk Rating	Recommendation	Agreed Yes/No	Management Response	Target
2. Policies and procedures are available to staff covering some parts of Information Governance and Data Protection, however these are spread throughout other policies, need updating. Some staff have difficulty locating them and there is a lack of understanding of personal responsibility. This situation does not offer sufficient strength for robust disciplinary responses in the case of breaches.	Multiple policies containing references to DP risks conflict of statement when policies are updated or amended at different times. The council also risks being unable to respond to breaches, with staff being unclear on responsibilities.	**M**	A comprehensive suite of basic, well structured Information Governance polices to be written and embedded into the organisation. Compliance with all policies should be monitored, and lack of adherence to them acted upon.	**Yes**	Work has already started on a review and redrafting of existing policies into a modular suite of discrete, but cross referenced policies. Information Security Policy Framework approved at CMT on 25th September along with priorities for policy development. **ON TARGET**	Policies all completed by **31/12/13**

ERP B - Data Protection Action Plan

	Observation	Risk	Risk Rating	Recommendation	Agreed Yes/No	Management Response	Target
3.	There are no explicit confidentiality or Data Protection compliance statements in staff contracts. Information Governance and Data Protection is not part of the routine operational management processes.	Difficulty in the organisation presenting a corporate response to staff who breach the Organisational Policy in line with legislation.	**H**	An addendum to staff contracts to include basic compliance statements with Confidentiality and Data Protection. Line Managers to embed Information Governance and Data Protection requirements in operational management processes.	**No**	The Council achieves contractual compliance through its policies that apply to all staff. **GREEN - COMPLETED**	**Linked to Policy Development**
4.	There is a lack of understanding of how Data Protection principles impact day to day activities in individual services, and the level of individual responsibility required by the DPA	The council risks local service level breaches through error. This carries risk of significant fines from the ICO	**M**	Annual staff training in Information Governance and Data Protection to ensure staff compliance and understanding of their responsibilities.	**Yes**	A new multimedia DP training suite has been deployed, and completion has been mandated by CMT. Service level needs will be assessed following reports of service by service completion. Services should annually assess DP issues to ensure that compliance, and ensure that appropriate training is available to staff to mitigate risks and address service specific issues. Basic corporate training for all staff should be maintained at a corporate level. Each service to develop its own induction to the data protection risks and controls for delivery to new team members, annual review of the content linked to the annual risk assessment. **ON TARGET**	**Completed** **31/03/13 and annually thereafter** **Completed and in place for induction and basic training** **12/12/13**

ERP B - Data Protection Action Plan

	Observation	Risk	Risk Rating	Recommendation	Agreed Yes/No	Management Response	Target
5.	There is a lack of formal records of procedures relating to data management	There is a risk that procedures will not be followed, or staff may introduce anomalies into processing workflows, resulting in DP breaches	**M**	Services produce maps of data moving into and out of their workflows, and produce formal procedure records on main tasks and work areas	**Yes**, on a risk based approach	There are significant resourcing implications for this recommendation so it will be undertaken on a risk based approach linked to the risk assessment of data protection compliance within each service. Key areas of risk will need to have information flows reviewed and appropriate controls evaluated. **NOT STARTED**	**31/03/14**
6.	Staff Intranet presents relevant DP policies in a number of different locations. Version control required	Without a coherent and structured presentation, there is a risk of confusion about which policy to follow, and that some policies may become out of date.	**M**	Intranet needs to be reviewed to ensure policies are up to date and accurate. The Structure needs to be addressed to ensure staff find it user friendly to locate policies	**Yes**	Intranet DP assets have been reviewed and a new DP section describing individual responsibilities has been launched. The new Information Security Policy framework will be held here, new policies added as they are developed and approved and cross linked to HR and IT sections. The HR policy template for is being used to ensure that review is built into the policy lifespan. **ON TARGET**	**31/03/13**
7.	Laptops have not been encrypted	Risk of client machine information being access by third parties in instances of theft or accidental loss.	**H**	All laptops to be recalled to ensure that encryption is installed as a matter of urgency.	**Yes**	Immediate action is being taken to secure relevant laptops. ITSG to receive report at every meeting regarding status and control of mobile devices, member's IT equipment and device encryption. **ON TARGET**	**31/05/13**

ERP B - Data Protection Action Plan

	Observation	Risk	Risk Rating	Recommendation	Agreed Yes/No	Management Response	Target
8.	Emails containing client sensitive data sometimes sent and received to and from outside the organisation without encryption. Information unsecured in transit.	Risk of interception or information sent to wrong recipient in error	**H**	Content encryption needs to be used when sending client identifiable and sensitive data outside the organisation and offered to customers sending information to the council.	**Yes**	Existing processes reviewed in a report to ITSG by IT to make best use of document level encryption. **NOT STARTED**	**31/03/13**
9.	Confidential Waste Bins: The bins for secure waste and ordinary waste are the same colour, shape and size	There is potential for them to be mixed up by staff using them.	**M**	Bins should be different colours or marked clearly.	**Yes**	This has already been undertaken, with confidential waste bins marked by a red lock covering, and non-confidential waste bins marked by a warning label **GREEN - COMPLETED**	**Completed**
10.	Visitors Sign In at main reception and should be issued a Visitor badge/sticker. This sometimes does not happen	Risk of unauthorised person being observed in the building, but mistaken for a legitimate visitor	**M**	The visitors system needs to be reviewed and compliance addressed to ensure that visitors wear Visitor badges whilst on site.	**Yes**	Supply of visitor badges reviewed. Visitor compliance to be addressed through SMG **GREEN - COMPLETED**	**Completed**
11.	Data Breach Policy and Procedures: The policy/procedure to follow regarding breaches is not widely understood	Risk of inconsistent reporting and lack of reporting of incidents	**M**	Data Breaches Policy should be reviewed and clearly integrated into general policies.	**Yes**	Breach Policy has been reviewed, and will be moved to the new Intranet DP section. **GREEN - COMPLETED**	**31/12/12**

ERP B - Data Protection Action Plan

Observation	Risk	Risk Rating	Recommendation	Agreed Yes/No	Management Response	Target
12. Consultations conducted without centralised control or oversight – varying degrees of understanding among those concerned about DP issues	Risk of non-standardised approaches and non-compliant processing leading to DP breaches	**M**	Notification of ANY consultations to the Consultation officer (Community Projects/Engagement) and Information Manager be mandatory and enforced at Directorate level. Review of Consultation Tool-kit to assure fit for purpose for assisting DP compliance	**Yes**	To be raised in Staff Briefing, SMG compliance. Is written in to existing policies for consultation. **GREEN - COMPLETED**	**31/12/12**

H – High Risk
M – Medium Risk
L – Low Risk