Zurich Information Governance Health Check - Management Action Plan

Area	No	Recommendation	Management Response	Implementation Date	Responsible Officer	Notes
Leadership & Management	1	Develop a corporate communications strategy around information governance which is recognised and supported at a local level.	Corporate Comms Strategy for information governance to be defined within Q4 2016/2017 and issued to SIRO for review before being issued for roll out in the next financial year	Q1/2 2017/2018	Sarah Slater SIRO	
	2	Review Corporate Risks 3, 13, 17 in the context of information incident response, disaster recovery and business continuity procedures delivering mitigation controls and capture on the risk register.	Corporate risks are reviewed on a Quarterly basis. The departmental risks for IG held within the Finance and IT directorate are reviewed monthly and feed into the Corporate register.	Completed	Sarah Slater Shane Agnew	SS and SA will continue to review the risks on a regular basis.

Area	No	Recommendation	Management Response	Implementation Date	Responsible Officer	Notes
	3	Provide clarity to Heads of Service regarding the recording of information governance risks on Departmental Risk Registers.	Intention for SIRO to introduce IAO training in Q1/2 of 2017/2018. This will incorporate the inclusion of IG risks on departmental registers	Q2 2017/2018	Sarah Slater SIRO	Issue will also be addressed at CRRF.
	4	The Council should review the opportunities from exploiting data as part of its annual review and planning cycle in the next 24 months.	Once the IAR has undergone a full review, the output from that register will drive out any assets that may contain opportunities for exploitation.	TBC	Sarah Slater	

Area	No	Recommendation	Management Response	Implementation Date	Responsible Officer	Notes
Strategy & Policy	5	Set target dates should be set for the completion of the Asset Registers. Monitor and report on progress to the SIRO/CRRF. Asset Owners should ensure both electronic and physical assets are considered. Asset Owners need to identify suitable review periods but must ensure a minimum annual review.	Review of IAR scheduled for Q4 2016/2017, with support from SIRO to encourage IAO and IAA to review and update their own areas. Updated SharePoint site will be published towards the end of Q1 2017/18.	Q1 2017/2018	Sarah Slater SIRO/IAO's	

Area	No	Recommendation	Management Response	Implementation Date	Responsible Officer	Notes
	6	The Acceptable Use Policy should be reviewed to ensure it remains relevant and fit for purpose against a backdrop of new ways of working and technology developments.	AUP has been reviewed. Intention is to issue this to Policy Working Group and the Unions for approval in Q4 2016/2017.	Q4 2016/2017	Sarah Slater	Roll out via MetaCompliance in Q4 2016/2017 with assistance from Comms.
People & Training	7	Create enhanced focus on information governance objectives by making explicit reference to individual responsibilities and performance within the annual appraisal process.	Work with HR to add this to HoS/Managers appraisal template	Q4 2016/2017	Sarah Slater	

Area	No	Recommendation	Management Response	Implementation Date	Responsible Officer	Notes
	8	Review training needs for staff with records management responsibilities (Business Support Managers) and consider Level 2 Protecting Information as mandatory for this group.	Reviewed RM responsibility across the high volume personal data areas. All Line managers with RM responsibility and all IAO's will be advised to complete Responsible for Information-IAO (Old Level 2) from next Financial year.	Q1 2017/2018	Sarah Slater	
	9	Design and implement an information security awareness program to enhance the security.	Information Security On-line training programme added to the courses on Me Learning in Q3 2016/2017. Approval from Deputy Chief Exec to instruct Mandatory from 2017/2018	Q1 2017/2018	Sarah Slater	Comms to be pushed out that Info Sec is mandatory at the same time as appraisal notifications.

Area	No	Recommendation	Management Response	Implementation Date	Responsible Officer	Notes
Technology & Infrastructure	10	Robustly and consistently implement the Clear Desk Policy and monitor performance through line management activities and audit processes.	Clear Desk Policy to be issued to Policy Working Group in Q4 2016/2017 with a view to a Comms MetaCompliance push in Q1 2017/2018	Q1 2017/2018	Sarah Slater/Comms	
	11	Developing and implement a data classification policy.	Classification Policy reviewed in line with Government Policy.	Q4 2016/2017	Sarah Slater	Policy will be uploaded to the IG pages of the Intranet. IAO will be issued with supporting documentation for cascade
	12	Improve understanding and application of document retention requirements for both physical and electronic records.	Retention schedule is refreshed on a quarterly basis with updated legislation. Look to implementing online guidance and training for retention within 2017/2018.	Q4 2017/2018	Sarah Slater	

Area	No	Recommendation	Management Response	Implementation Date	Responsible Officer	Notes
	13	Information assets held on network shares need to be identified and suitable controls to manage access at the required level implemented.	All Core System Data Assets held on network shares are managed by permissioned access control following a period of user training. Other ad-hoc systems held on network shares will be reviewed as part of the IAR Review which begins in Q4 2016/2017. Once the Asset Register has been defined, data access controls and data flows will be added.	Q1 2017/2018	Sarah Slater	
	14	Consider developing a campaign aimed at challenging the need to print and encouraging a "think before you print" culture.	Comms (Business Analyst team in IT) to pick this up as part of the revamped CADS process.	TBC	Alison Smith	

Area	No	Recommendation	Management Response	Implementation Date	Responsible Officer	Notes
Supply Chain	15	The Council needs to further develop procedures, guidance and awareness to ensure Contract Managers and Commissioners are obtaining sufficient assurance that third parties are meeting their information governance and business continuity contractual obligations.	Review of Corporate 3rd party contracts as part of GDPR implementation includes redraft of Data Processor Agreements and Information Sharing Agreements. Once this documentation reflects the requirements of best practice and GDPR implementation, this will be cascaded to relevant staff members	Q2/3 2017/2018	Sarah Slater IAOs SIRO Legal Services	

Area	No	Recommendation	Management Response	Implementation Date	Responsible Officer	Notes
	16	Develop a consistent approach to obtaining informed consent from Service Users to ensure data can be suitably shared across BwD and, where relevant, its partners, to support delivery of improved outcomes.	The new GDPR includes specific definition of consent that was lacking in the DPA. Implementation of GDPR and best practice of this will filter through to the revision of data collection forms that will be required in order to comply.	2017/2018	Sarah Slater	This will be an ongoing process to firstly identify all the Councils data collection processes before revising to reflect the requirements of the GDPR which need to be implemented by 2018.
Incident Management	17	Undertake a business continuity exercise around a Cyber / Information Risk scenario to test existing arrangements. This will highlight any potential weaknesses and allow mitigation or developments of the plans to take place.	This will be happening in February 2017 at the managers meeting, the next corporate theme exercise will be bases around cyber risk.	Q4 2016/2017	Civil Contingencies	

Area	No	Recommendation	Management Response	Implementation Date	Responsible Officer	Notes
	18	Services Managers should ensure reporting arrangements within their Teams respond adequately to "out of hours" incidents.	Data Security and breach handling procedures have been published to the IG Intranet page. Cascade will be issued to IAO in CRRF, with instructions to inform relevant staff members.	Q4 2016/2017	Sarah Slater	CF to add to next CRRF Agenda.
	19	Service Managers should be provided with guidelines to support them in responding to an initial data breach incident ensuring that key information is collected and suitable actions are taken to mitigate the loss.	As above	Q4 2016/2017	Sarah Slater	CF to add to next CRRF Agenda.

Area	No	Recommendation	Management Response	Implementation Date	Responsible Officer	Notes
Audit and Compliance	20	To improve oversight, Audit Committee should be encouraged to periodically select a key Corporate Risk and undertake a deep dive into its assessment, control and monitoring. A key Officer for the subject area should be invited to attend the meeting.	The Audit & Governance Committee will be asked to select a corporate risk for consideration at each meeting. The Risk Owner or Key Contact will be invited to attend the Committee meeting for the Committee to discuss the details recorded in the risk entry including the risk assessment, controls identified and monitoring arrangements.	April 2017	Colin Ferguson	

Area	No	Recommendation	Management Response	Implementation Date	Responsible Officer	Notes
	21	Consider developing a framework facilitating a proportionate and risk based approach designed to provide assurance to BwD on the management of information risk in suppliers of services to the Council.	The GDPR proposes ‘Privacy by design’. This will incorporate risk assessments for Information assets at the beginning of every procurement process as part of the mandatory Privacy Impact Assessment process. Steps already in place to ensure this mandatory process is in place before 2018.	2017/2018	Sarah Slater	

Area	No	Recommendation	Management Response	Implementation Date	Responsible Officer	Notes
	22	Consideration should be given to implementing a planned programme of site audits to assess the strength of information security practice. The process, as well as driving improvement, would also provide a further source of control assurance.	Consideration will be given to this requirement following review of resource requirements within the IG team in 2017/2018	2017/2018	Sarah Slater	