Corporate Information Governance Group

Level 1 Information Maturity Model Action Plan

Ref	High Level Action	Ref	Action and Current Position	By	Date	RAG
1	Promulgate top level policy statement • Publish Information Charter	a	Review and update Information Charter – ensure it aligns to the IAMM	RP	06/13	I/P
		b	Obtain CMT approval for Charter	IF	08/13	
		c	Develop comprehensive list of Information Governance policies	RP/RB	08/13	
2	Senior commitment to Information Assurance • Appoint Senior Information Risk Owner (SIRO) • Report to Main Board regularly • Provide assurance to Audit Committee on annual basis		*SIRO appointed and sits on Main Board. Reports to CMT and Audit Committee as part of annual reporting cycle.*		✓	I/P
		a	Annual progress report to CMT	IF	04/13	
		b	Annual assurance report to Audit Committee	RP	04/13	
		c	Develop assurance mechanism to support SIRO assurance report	RP	10/13	
3	Appoint Information Asset Owners (IAOs) for each key group of information assets		*Information Asset Groups identified and communications established. 50 key IAOs used as basis for communication*		✓	I/P
		a	Continue ongoing awareness training of the key "50" information asset owners	RB	Ongoing	
		b	Review information asset registers and ensure "fit for purpose"	RB	Ongoing	
4	Develop reporting mechanism to provide assurance to SIRO • Breach reporting and investigating system • IAO assurance to SIRO • Compliance review	a	Review and update Data Breach reporting mechanism	RP	06/13	I/P
		b	Develop assurance mechanism for IAOs to feed into DIGCs and annual assurance as part of SIC (see 2c)	RB	10/13	
		c	Carry out reviews of adherence to Data Breach policy as part of audit programme - Included in audit programme 13/14	RP	✓	
		d	Carry out QA reviews of FoI cases and report to CIGG quarterly	RB	Ongoing	
		e	Develop and implement file management standards to ensure compliance with Legal Admissibility Code of Practice	PH	10/13	
		f	Carry out compliance reviews of adherence to LA Code of Practice. Report annually to CIGG and include in annual assurance to Audit	PH/RP	04/14	

Ref	High Level Action	Ref	Action and Current Position	By	Date	RAG
			Committee			
5	Carry out annual risk awareness training for those with access to personal data • Identify groups of staff and their training needs • Develop training packs for different groups • Deliver selected training • Monitor delivery of training	a	Continue Shout campaign – include findings from internal audit visits in campaign	RP/RB	Ongoing	**I/P**
		b	Conduct spot checks of compliance with security in West offices	RP	Ongoing	
		c	Develop and implement Metacompliance	RP/RG	06/13	
		d	Identify training needs of different groups of staff	DIGCs	06/13	
6	Develop data sharing protocols with 3rd party suppliers & delivery partners • Identify groups, exposure and needs • Develop appropriate awareness information packs • Ensure requirement is included in contracts • Deliver training where appropriate	**a**	Ensure robust data sharing protocols exists with partners operating from the new CYC offices	RB	05/13	**I/P**
		b	Review CYC arrangements against NHS data sharing standards	RB	05/13	
		c	Identify and review all partnerships to ensure protocols are in place	RB	06/13	
7	Develop Information Risk Policy • Define information risk appetite • Agree classification scheme for records • Communicate scheme to staff • Monitor compliance		*Classification scheme in place and communicated to staff via Colin*		✓	**I/P**
		a	Conduct QA reviews of Information Asset registers and application of classification scheme	RB	10/13	
		b	Develop and implement records management policy	PH	11/13	
		c	Implement Legal Admissibility policy	PH	11/13	
		d	Develop assurance mechanism for BS 10008	RP/PH	10/13	
8	Develop Information Risk Register • Register monitored regularly • Highest risks fed into corporate risk register • IAOs and IMs identified in Information Risk Registers	a	Develop Information risk register	RP/ RB	07/13	**I/P**
		b	Ensure key DP risks are considered as part of business risk register for CYC	RP	07/13	
9	Information Security • Develop Information Security Policy covering both IT and non IT based data • IT Security Officer appointed • Access to and use of sensitive data monitored	a	Develop policy for home working and bring your own devices	RG	06/13	**I/P**
		b	Submit BYOD and Home Working policies to CIGG and CMT for approval	RG	08/13	
		c	Review arrangements for IT security compliance monitoring	RP	08/13	
		d	Monitor EDRMS Info Gov security arrangements	CIGG	Ongoing	
10	Data/Information Transparency	a	Review Compliance with Code of Practice – Self Assessment	CIGG	08/13	**I/P**