Ref	Category	Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Jul 2014	Likelihood before mitigations Jul 2014	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jul 2014		RISK score after Mitigation Jan 2014
	Operations SO1.GG SO2.EBP	2.10	Telephone system failure causing protracted service outage	Director of IT	4	3	**12**	Support and maintenance contract for hardware and software of the ACD and PABX	Backup of the configuration for both the ACD and PABX	Diverse routing for the physical telephone lines from the two exchanges with different media types	Low		Low
5	**IT SO2.EBP SO1.GG**	5.1	Software Virus damage	Director of IT	4	5	**20**	Anti-virus software deployed at several key points. Perimeter controls enabled.	Adherence to IT policy, procedures and training	Regular externally run security penetration tests.	Low		Low
	IT SO2.EBP SO1.GG	5.2	Technology obsolescence, (Hard/SoftWare)	Director of IT	2	2	4	Delivery of the IT strategy including the refresh of technology.	Employ small core of mainstream technology with recognised support and maintenance agreements	Accurately record technology assets.	Low		Low
	IT SO2.EBP SO1.GG	5.3	Fraud committed through IT services	Director of IT	3	3	9	Appropriate and proportionate access restrictions to business data. System audit trails.	Regular, enforced strong password changes.	Regular externally run security tests.	Low		Low
	IT SO2.EBP SO1.GG	5.4	Failure of IT Continuity Provision	Director of IT	4	3	**12**	Annual IT continuity tests	IT continuity plan is reviewed when a service changes or a new service is added	Appropriate and proportionate technical solutions are employed. IT technical staff appropriately trained.	Low		Low
	IT SO2.EBP SO1.GG	5.5	Malicious damage from unauthorised access	Director of IT	4	2	8	Security is designed into the IT architecture, using external expert consultancy	Regular externally run security penetration tests.	Periodic and systematic proactive security reviews of the infrastructure. Application of security patches in a timely manner. Physical access to the IT infrastructure restricted and controlled.	Low		Low
	IT SO2.EBP SO1.GG	5.6	Data service disruption (via utility action)	Director of IT	5	1	5	Redundant services	Diverse routing of services where possible	Appropriate service levels with utility providers and IT continuity plan	Low		Low
	Education SO1.GG	7.5	Education database failure	Director of IT	3	2	6	Effective backup and recovery processes	In house and third party skills to support system	Included in future DR/BC tests	Low		Low
	Registration SO2.EBP SO3.Com	10.2	Protracted service outage following a NetRegulate Registration system failure	Director of IT	5	3	**15**	Effective backup and recovery procedures	Maintenance and support contracts for core system elements.	Annual IT Continuity tests	Low		Low
	Fitness to Practise SO2.EBP SO1.GG	13.10	Protracted service outage following a Case Management System failure	Director of IT	5	3	**15**	Effective backup and recovery procedures	Maintenance and support contracts for core system elements	Annual IT continuity tests	Low		Low
	Information Security SO1.GG SO2.EBP	17.1	Electronic data is removed inappropriately by an employee	Director of IT	5	3	**15**	Employment contract includes Data Protection and Confidentiality Agreement	Adequate access control procedures maintained. System audit trails.	Laptop encryption. Remote access to our infrastructure using a VPN . Documented file encryption procedure	Low		Low

	Information Security SO1.GG SO2.EBP	17.3	Loss of electronic data	EMT, Director of IT and Director of Operations	5	3	**15**	Access is restricted to only the data that is necessary for the performance of the services.	Effective system processes including secure data transfer and remote access granted only on application and through secure methods. Training where appropriate Employees & (Partners)	Data Processor agreements signed by the relevant suppliers.	Low		Low
	Information Security SO1.GG SO2.EBP	17.6	Loss of Registrant personal data by the registration system (NetRegulate) application support provider in the performance of their support services (specific risk).	Director of IT and Director of Operations	5	3	**15**	Access to and export of Registrant data is restricted to only that which is necessary for the performance of the services.	Effective system processes including secure data transfer and remote access granted only on application and through secure methods.	Data processor side letter specifying obligations and granting a limited indemnity.	Low		Low