ASSET	RESPONSIBILITY	ASSET VALUE	Threat description	Threat value	Control description	Control value	Total Risk Value	Residual
Information Assets : database's & data files, other files & copies of plans, system documentation, original user manual's, original training material, operational or other support procedures, continuity plans & other fall-back arrangements, archived information, financial & accounting information.								
Virtual Servers	GB	10	**Unintentional** **Unable To Access.** **Accidental Loss/Damage.** **System/Service Failure.**	3	Firewall, Network access controls. Physical security 24/7. Segregation of responsibilities and control of administrator privileges.	1.5	45	
	GB	10	**Intentional** **Malicous Damage/Fraud.** **Theft (Internal/External)** **Unauthorised Access** **DDoS**	4	Firewall, Network access controls. Physical security 24/7. Segregation of responsibilities and control of administrator privileges.	1.5	60	
Email	GB		**Loss of access to email, internally and externally including sent/received documents**					
	GB	9	**Unintentional** **Unable To Access.** **Accidental Loss/Damage.** **System/Service Failure.**	3	Back-ups and procedures. Email policy. Physical security 24/7. Segregation of responsibilities and control of administrator privileges.	2	54	
	GB	9	**Intentional** **Malicous Damage/Fraud.** **Theft (Internal/External)** **Unauthorised Access** **DDoS**	3	Anti-spyware, content filtering, Anti-virus. Email Policy, Firewall. Physical security 24/7. Segregation of responsibilities and control of administrator privileges.	2	54	
Database Server	GB	10	**Loss of access to reporting tools**					
	GB	10	**Unintentional** **Unable To Access.** **Accidental Loss/Damage.** **System/Service Failure.**	2	Back-ups, firewall, Anti-virus, Anti-spyware, security groups, group policies. Segregation of responsibilities and control of administrator privileges.	0.75	15	
	GB	10	**Intentional** **Malicous Damage/Fraud.** **Theft (Internal/External)** **Unauthorised Access** **DDoS**	2	Back-ups, firewall,Anti-virus, Anti-spyware, security groups, group policies. Physical security 24/7. Segregation of responsibilities and control of administrator privileges.	0.75	15	
Electronic Document Storage	GB							
File server	GB	10	**Loss of current and historical documents, including (but not limited to) electronic copies of letters, manuals, review documents, proposals, contracts.**					
	GB	10	**Unintentional** **Unable To Access.** **Accidental Loss/Damage.** **System/Service Failure.**	3	Back-ups, firewall, Anti-virus, Anti-spyware, security groups, group policies. No document management system to improve accessibility, retrieval of docs and accidental loss. Physical security 24/7. Segregation of responsibilities and control of administrator privileges.	1.5	45	
	GB	10	**Intentional** **Malicous Damage/Fraud.** **Theft (Internal/External)** **Unauthorised Access** **DDoS**	3	Back-ups, firewall, Anti-virus, Anti-spyware, security groups, group policies. Physical security 24/7. Segregation of responsibilities and control of administrator privileges.	1.5	45	
Dropbox	GB	10	**Loss of current and historical documents, including (but not limited to) electronic copies of letters, manuals, review documents, proposals, contracts.**					

ASSET	RESPONSIBILITY	ASSET VALUE	Threat description	Threat value	Control description	Control value	Total Risk Value	Residual
	GB	8	Unintentional Unable To Access. Accidental Loss/Damage. System/Service Failure.	5	Back-ups, Anit-virus, Anti-spyware. No document management system to improve accessibility, retrieval of docs and accidental loss.	2	80	
Intranet/CRM/Helpdesk/IT Support Tools	GB		Intranet (Loss of internal communication and document access) / CRM (Loss of client contact management data, sales prospect/lead data) / Helpdesk (loss of access to online booking system) / IT Support tools (Loss of access to internal support tools)					
	GB	5	Unintentional Unable To Access. Accidental Loss/Damage. System/Service Failure.	3	Back-ups, firewall,Anti-virus, Anti-spyware, security groups, group policies. Record assets with all the relevant info about the asset. Physical security. Secure logins and controls over access levels - managed witihn the apllication.	3	45	
	GB	5	Intentional Malicous Damage/Fraud. Theft (Internal/External) Unauthorised Access DDoS	3	Back-ups, firewall, Anti-virus, Anti-spyware, security groups, group policies. Record assets with all the relevant info about the asset. Physical security. Secure logins and controls over access levels - managed witihn the apllication.	3	45	
Other Electronic Data Sources	GB							
Network	GB		Loss of access to internal network					
	GB	10	Intentional Malicous Damage/Fraud. Theft (Internal/External) Unauthorised Access	2	Secure network access (ACS), Segregation of duties for network equipment, limited/controlled access, physical security .	2	40	
	GB	10	Unintentional Unable To Access. Accidental Loss/Damage. System/Service Failure.	4	Secure network access (ACS), Segregation of duties for network equipment, limited/controlled access, physical security , resilience i.e. Duplicatiion/replication/redundancy	2	80	
Internet (ISP)	GB		Loss of to external network access including (but not limited to) internet, online bookings, email					
	GB	10	Unintentional Unable To Access. Accidental Loss/Damage. System/Service Failure.	4	Multiple ISP connections with automatic failover if one fails.	2	80	
	GB	10	Intentional Malicous Damage/Fraud. Theft (Internal/External) Unauthorised Access	3	Equipment is housed in secure cabinets which are kept locked. Keys are stored securely in a locked cabinet. Spare equipment is on hand to replace equipment that is damaged/stolen	1.75	52.5	
Backup Components	GB	9	Intentional Malicous Damage/Fraud. Theft (Internal/External) Unauthorised Access	2	Back up processes and procedures, checklist, off site storage, physical controls, test processes.	2	36	
	GB	9	Unintentional Unable To Access. Accidental Loss/Damage. System/Service Failure.	2	Back up processes and procedures, checklist, off site storage, physical controls, test processes.	2	36	
Software Assets : application software, system software, development tools & utilities, e-Learning assets, network tools & utilities								

ASSET	RESPONSIBILITY	ASSET VALUE	Threat description	Threat value	Control description	Control value	Total Risk Value	Residual
Operating Systems	GB	9	**Intentional** **Malicous Damage/Fraud.** **Theft (Internal/External)** **Unauthorised Access**	2	Back-ups, firewall, Anti-virus, Anti-spyware, security groups, group policies. Record assets with all the relevant info about the asset. Physical security controls.	2	36	
	GB	9	**Unintentional** **Unable To Access.** **Accidental Loss/Damage.** **System/Service Failure.**	3	Back-ups, firewall, Anti-virus, Anti-spyware, security groups, group policies. Record assets with all the relevant info about the asset. Physical security controls.	2	54	
Finance System	GB / DB		**Loss of access to financial system for generating invoices and purchase orders**					
	GB / DB	9	**Intentional** **Malicous Damage/Fraud.** **Theft (Internal/External)** **Unauthorised Access**	2	Back-ups, firewall, Anti-virus, Anti-spyware, security groups, group policies. Record assets with all the relevant info about the asset. Physical security. Application is protected by authauntication - passwrod protected - only accesible by Finance Team.	2	36	
	GB / DB	9	**Unintentional** **Unable To Access.** **Accidental Loss/Damage.** **System/Service Failure.**	3	Back-ups, firewall, Active directory, Anti-virus, Anti-spyware, security groups, group policies. Record assets with all the relevant info about the asset. Physical security. Application is rotected by authauntication - passwrod protected - only accesible by Finance Team.	2	54	
General Productivity Tools: MS Office, Word, Excel, PowerPoint, Outlook	GB		**Impact on all areas of business**					
	GB	2	**Unintentional** **Unable To Access.** **Accidental Loss/Damage.** **System/Service Failure.**	3	Licensing, physical and logical security measures, lack of controls of password management of the tools.	2	12	
	GB	2	**Intentional** **Malicous Damage/Fraud.** **Theft (Internal/External)** **Unauthorised Access**	3	Licensing, physical and logical security measures, lack of controls of password management of the tools.	2	12	
Phone system	GB		**Loss of inbound and outbound telephone calls**					
	GB	3	**Intentional** **Malicous Damage/Fraud.** **Theft (Internal/External)** **Unauthorised Access**	2	Physical security 24/7. Divert to mobile.	2	12	
	GB	3	**Unintentional** **Unable To Access.** **Accidental Loss/Damage.** **System/Service Failure.**	3	Physical security 24/7. Divert to mobile. Review additional controls again with telecoms provider	4	36	
IT Development Tools -Code editors, compilers, ide environments	GB		**Loss of core development tools - impacting ability to provide continued development, maintenance and support for business**					
	GB	2	**Intentional** **Malicous Damage/Fraud.** **Theft (Internal/External)** **Unauthorised Access**	3	Back-ups, firewall, Anti-virus, Anti-spyware, security groups, group policies. Record assets with all the relevant info about the asset. Physical security. Secure logins and controls over access levels - managed witihn the apllication.	3	18	

ASSET	RESPONSIBILITY	ASSET VALUE	Threat description	Threat value	Control description	Control value	Total Risk Value	Residual
	GB	2	**Unintentional** **Unable To Access.** **Accidental Loss/Damage.** **System/Service Failure.**	3	Back-ups, firewall, Anti-virus, Anti-spyware, security groups, group policies. Record assets with all the relevant info about the asset. Physical security. Secure logins and controls over access levels - managed witihn the apllication.	3	18	
	GB							
Detailed Asset Register Listing available	GB		**Loss of IT infrastructure, services and associated data.**					
Servers	GB	10	**Intentional** **Malicous Damage/Fraud.** **Theft (Internal/External)** **Unauthorised Access**	3	Physically Secured data centre. swipecard entry restricted to designated IT employees only. 24x7 monitoring.	2	60	
	GB	10	**Unintentional** **Unable To Access.** **Accidental Loss/Damage.** **System/Service Failure.**	3	Physically Secured data centre. swipecard entry restricted to designated IT employees only. 24x7 monitoring.	2	60	
PC's	GB	7	**Intentional** **Malicous Damage/Fraud.** **Theft (Internal/External)** **Unauthorised Access**	3	All PC's recorded in Asset Register. Secure building access policy.	2	42	
	GB	7	**Unintentional** **Unable To Access.** **Accidental Loss/Damage.** **System/Service Failure.**	3	Acceptable use of IT policy and procedures Issues raised with the Service Desk. Under warranty.	3	63	
Laptop's/Portable computing devices	GB	7	**Intentional** **Malicous Damage/Fraud.** **Theft (Internal/External)** **Unauthorised Access**	3	Laptops only issued to employees who need them. Password policy in place to protect data in event of theft or loss. Remote access for backing up critical data to network.	4	84	
	GB	7	**Unintentional** **Unable To Access.** **Accidental Loss/Damage.** **System/Service Failure.**	3	Remote access and Dropbox for backing up critical data to network. Insurance for lost/stolen laptops. Under warranty.	3	63	
Monitors	GB	3	**Intentional** **Malicous Damage/Fraud.** **Theft (Internal/External)** **Unauthorised Access**	3	All monitors recorded in Asset Register. Secure building access policy.	3	27	
	GB	3	**Unintentional** **Unable To Access.** **Accidental Loss/Damage.** **System/Service Failure.**	3	Acceptable use of IT policy. Warranty and insurance.	2	18	
Printers / Scanner	GB	3	**Intentional** **Malicous Damage/Fraud.** **Theft (Internal/External)** **Unauthorised Access**	3	All printers recorded in Asset Register. Standard printers utilised for ease of maintenance/replacement/support. Physical building policy. 24x7 monitoring.	3	27	
	GB	3	**Unintentional** **Unable To Access.** **Accidental Loss/Damage.** **System/Service Failure.**	3	Internal IT Support with full hardware maintenance contract. Standard printers utilised thoughout for easy maintenance/replacement. 24x7 monitoring.	3	27	
Routers & Switches & Firewalls	GB	10	**Intentional** **Malicous Damage/Fraud.** **Theft (Internal/External)** **Unauthorised Access**	3	Physically Secured data centre swipe card entry restricted to designated IT employees only. Fully monitored via Munin Monitoring system.	3	90	

ASSET	RESPONSIBILITY	ASSET VALUE	Threat description	Threat value	Control description	Control value	Total Risk Value	Residual
	GB	10	**Unintentional** **Unable To Access.** **Accidental Loss/Damage.** **System/Service Failure.**	3	Physically Secured data centre swipe card entry restricted to designated IT employees only. Fully monitored via Munin Monitoring system.	2	60	
Phones	GB	3	**Intentional** **Malicous Damage/Fraud.** **Theft (Internal/External)** **Unauthorised Access**	3	All phones recorded in the Asset Register. Physical buidling policy.	3	27	
	GB	3	**Unintentional** **Unable To Access.** **Accidental Loss/Damage.** **System/Service Failure.**	3	All phones recorded in the Asset Register. Physical buidling policy.	3	27	
Mobile phones	GB	3	**Intentional** **Malicous Damage/Fraud.** **Theft (Internal/External)** **Unauthorised Access**	4	All phones recorded in Asset Register. Password protected. Ease of replacement. Centrally managed with ability to lock/wipe phone if lost/stolen.	3	36	
	GB	3	**Unintentional** **Unable To Access.** **Accidental Loss/Damage.** **System/Service Failure.**	4	All phones recorded in Asset Register. Password protected. Ease of replacement. Centrally managed with ability to lock/wipe phone if lost/stolen.	4	48	
USB devices	GB	5	**Intentional** **Malicous Damage/Fraud.** **Theft (Internal/External)** **Unauthorised Access**	4	Encryption used where required. Removable Media Policy	3	60	
	GB	5	**Unintentional** **Unable To Access.** **Accidental Loss/Damage.** **System/Service Failure.**	5	Removable Media Policy	3	75	
UPS	GB	7	**Intentional** **Malicous Damage/Fraud.** **Theft (Internal/External)** **Unauthorised Access**	3	Located in secure Computer room (IT Staff Only). UPS devices monitored by IT Team. Data centre UPS features redundancy and backup diesel generators	2.5	52.5	
	GB	7	**Unintentional** **Unable To Access.** **Accidental Loss/Damage.** **System/Service Failure.**	3	Dual power supply to Computer room - load balancing of key servers/devices.	2.5	52.5	
Air-Conditioning (Computer)	GB	7	**Intentional** **Malicous Damage/Fraud.** **Theft (Internal/External)** **Unauthorised Access**	3	Located in secure Computer room (IT Staff Only).	3	63	
	GB	7	**Unintentional** **Unable To Access.** **Accidental Loss/Damage.** **System/Service Failure.**	3	For GRDC data centre, SLA in place with colocation provider for provision of HVAC environment.	3	63	
Environmental								

ASSET	RESPONSIBILITY	ASSET VALUE	Threat description	Threat value	Control description	Control value	Total Risk Value	Residual
Property/building	GB	8	Intentional/Unintentional	4	Multi-tenanted occupancy, covering 1st floor. Floor plans available. The buildings and contents are insured. H & S and security Policy and Procedures in place. Good access to the building re. travel links. A Fire Assessent has been conducted. Assessment regarding other environmental threats have been considered and controls been put in place i.e. siting of equipment. Controls are in place by building security and office entry is via key fob. All offices should be locked outside of office hours. Any potential secuity breach should be raised with GB. If unable to access the buildings then back-ups are in place capability exists to support remote working.	2	64	
Desks/seating for staff/visitors	GB	2	Intentional/Unintentional	2	Desks and seating for staff where posible are located to maximise space and privacy	4	16	
Air-Conditioning	GB	5	Intentional/Unintentional	5	Air conditioning units vent to be kept clear of paperwork/cluter to prevent malfunction. AC units tested regularly. There is an AC unit in the Server room which has been tested and is regularly maintained.	2	50	
Electrical								
Stationary inc. calculators Desk Fans	GB	1	Intentional/Unintentional	3	Secure 24/7 environment	4	12	
Photo-copiers/fax machines	GB	2	Intentional/Unintentional	3	Secure 24/7 environment	4	24	
Shredder	GB	2	Intentional/Unintentional	3	Secure 24/7 environment	4	24	
Reputation	BC	8	**Unintentional/Intentional**	3	Brand guidelines, controls over intranet and internet. Guidelines created for staff. Maintain links with industry journalists. Designated spokespersons to respond to press enquiries.	3	72	
Brand	BC	8	**Unintentional/Intentional**	3	Brand guidelines, controls over intranet and internet. Guidelines created for staff. Maintain links with industry journalists. Designated spokespersons to respond to press enquiries.	3	72	
Service	BC	8	**Unintentional/Intentional**	3	Brand guidelines, controls over intranet and internet. Guidelines created for staff. Maintain links with industry journalists. Designated spokespersons to respond to press enquiries.	3	72	
Physical Documents & Information Sources								

ASSET	RESPONSIBILITY	ASSET VALUE	Threat description	Threat value	Control description	Control value	Total Risk Value	Residual
Marketing								
Unpublished marketing data	LL	5	**Intentional** **Malicous Damage/Fraud.** **Theft (Internal/External)** **Unauthorised Access**	2	Internal marketing team is responsible for release of material to PR agencies. Material is stored in Dropbox and source code repository	3	30	
	LL	7	**Unintentional** **Unable To Access.** **Accidental Loss/Damage.** **System/Service Failure.**	2	IT controls - data backed up. Info transferred by email. Clear instructions on the approval process.	3	42	
Press releases, marketing literature, references, presentation, client/sovereign logo's	LL	5	**Intentional/Uninterntional** **Malicous Damage/Fraud.** **Theft (Internal/External)** **Unauthorised Access**	1	Central folder available for all staff - Good version control in place to avoid misuse. Quality controld over hard and soft copies. Marketing lierature controlled by Marketing department only.	3	15	
supplier contracts,	LL	5	**Intentional/Uninterntional** **Malicous Damage/Fraud.** **Theft (Internal/External)** **Unauthorised Access**	2	Stored in Excel IT Supplier list spreadsheet in Dropbox	7	70	
Website/intranet content	LL	8	**Intentional** **Malicous Damage/Fraud.** **Theft (Internal/External)** **Unauthorised Access**	3	Content is managed via revision control and hosted securely. An online CMS is *not* used so modififcation is not easy. All web content is encrypted and internal data is protected by username and password	2	48	
	LL	8	**Unintentional** **Unable To Access.** **Accidental Loss/Damage.** **System/Service Failure.**	2	Approval process to prevent misuse	3	48	
Budgets	BC/DB	6	**Unintentional** **Unable To Access.** **Accidental Loss/Damage.** **System/Service Failure.**	4	Managed by BC and DB and approval given to selected staff members	2	48	
Business Development								
Proposals	BC	5	**Intentional** **Malicous Damage/Fraud.** **Theft (Internal/External)** **Unauthorised Access**	2	Documents stored on DropBox that is shared by internall staff. Low Risk - employees saving data to desktops as they utilise dropbox. Control required to remind staff about restricting saving data to desktop. Office is locked. Hard copy docs should not be taken home or left in cars.	2	20	
	BC	5	**Unintentional** **Unable To Access.** **Accidental Loss/Damage.** **System/Service Failure.**	4	As above. Review of proposal and sign off before distribution to clients. Proposals marked as commercial in confidence.	2	40	
Performance reports (SLA)	GB	2	**Intentional** **Malicous Damage/Fraud.** **Theft (Internal/External)** **Unauthorised Access**	2	Certain SLA reports are published publically. Internal reports are held inside monitoring systems on the intranet	3	12	

ASSET	RESPONSIBILITY	ASSET VALUE	Threat description	Threat value	Control description	Control value	Total Risk Value	Residual
	GB	2	**Unintentional** **Unable To Access.** **Accidental Loss/Damage.** **System/Service Failure.**	2	As above	3	12	
HR								
Hard copy files in personnel filing cabinet include: Contracts, application forms, medical forms, cv's, pre-contract forms, copies of certificates, appraisal forms, leavers forms, induction evaluation forms, employee salary review and disciplinary records.	JW	2	**Malicious damage/fraud. Theft. Wilful damage.**	3	Locked filing cabinets. JW has access.	3	18	
	JW	2	**Unable to access**	4	Soft copies available - restricted access.	3	24	
	JW	2	**Accidental loss/damage. Disclosure of information. Breach of legislation i.e. Data protection Act.**	4	Soft copies available - restricted access.	2	16	
	JW	2	**Unauthorised access.**	4	Information Security controls.	3	24	
Employee details including: Personal contact details, dept, payroll, NI number, date of birth, leaving details, emergency contacts, holidays, absence and bank details.	JW	8	**Malicious damage/fraud/Theft**	4	Information is held at our accountants in addition to JW	2	64	
Finance								
P/L Inv Credit card statements Bank Statements/Letters Remits Credit card receipts Management Information Stats Finance Records, e.g. GP, MF Processes Payroll Insurance Bank Forms HMRC correspondance Disputes Leases/ CAPEX Statutory Records	DB	7	**Intentional** **Malicous Damage/Fraud.** **Theft (Internal/External)** **Unauthorised Access**	4	Locked filing cabinets. Physical security of the building. Electronic records are backed up. Access to registry financial reports is controlled.	2	56	
Misc								
Risk assessments	IST	4	**Intentional/Unintentional**	3	Copies are held in Dropbox and so are distributed among IST members.	4	48	
Reception record book	JW	2	**Intentional/Unintentional**	4	Office manned during office hours and locked otherwise. Completed pages are archived in a locked filing cabinet.	4	32	
Disaster Recovery Plan	IST	4	**Intentional/Unintentional**	3	Copies are held in Dropbox and so are distributed among IST members. Hard copies distributed to IST members to keep at home.	4	48	
Maintenance agreements	GB	3	**Intentional/Unintentional**	4	Agreements are controlled via designated managers	4	48	
Subscriptions to magazine/press/professional bodies	JW	1	**Intentional/Unintentional**	1	Reception manages the subscriptions	7	7	
Outsource suppliers	DB	7	**Intentional** **Malicous Damage/Fraud.** **Theft (Internal/External)** **Unauthorised Access**	3	Locked filing cabinets.	2	42	

ASSET	RESPONSIBILITY	ASSET VALUE	Threat description	Threat value	Control description	Control value	Total Risk Value	Residual
DropBox	GB	7	**Intentional** **Malicous Damage/Fraud.** **Theft (Internal/External)** **Unauthorised Access**	5	Dropbox provides version control and restoration from backups. Files are stored on each person's computers and "in the cloud." Files on the Dropbox website are protected by a username and password.	2	70	
Cryptographic Material & Credentials	GB	8	**Intentional** **Malicous Damage/Fraud.** **Theft (Internal/External)** **Unauthorised Access**	6	Cryptographic Policy in place. High value keys are stored on HSM/TPM devices as required. Other keys are backed up with multiple layers of encryption	2	96	
Petty Cash	JW	7	**Intentional** **Malicous Damage/Fraud.** **Theft (Internal/External)** **Unauthorised Access**	5	Locked filing cabinet.	2	70	
Business Systems								
5 Critical Services as defined by ICANN								
Shared Registry System	GB	10	**Intentional/Accidential** **ACCIDENTAL LOSS/DAMAGE** **UNAUTHORISED ACCESS** **SYSTEM/SERVICE FAILURE**	6	Physical security of server, firewalls, access control, logging/monitoring, resiliance to hardware/network failure	1	60	
Whois Service	GB	10	**Intentional** **Malicous Damage/Fraud.** **Theft (Internal/External)** **Unauthorised Access**	7	Physical security of server, firewalls, access control, logging/monitoring, resiliance to hardware/network failure. Rate limiting (abuse preventivie measures).	1	70	
Authoritative DNS Service	GB	10	**Intentional** **Malicous Damage/Fraud.** **Theft (Internal/External)** **Unauthorised Access**	10	Physical security of server, firewalls, access control, logging/monitoring, resiliance to hardware/network failure. Overprovisining to withstand Ddos attackts. Use of Tsig (transaction signature) and VPN to prevent tampering of zone data. Use of anycast to provide load balancing and isolation of attacks.	1	100	
DNSsec signing system	GB	10	**Intentional** **Malicous Damage/Fraud.** **Theft (Internal/External)** **Unauthorised Access**	5	Physical security of server, firewalls, access control, logging/monitoring, resiliance to hardware/network failure. Securing of cryptographic material (keys).	1	50	
Zone File Access System	GB	10	**Intentional** **Malicous Damage/Fraud.** **Theft (Internal/External)** **Unauthorised Access**	3	Physical security of server, firewalls, access control, logging/monitoring, resiliance to hardware/network failure	1	30	