<table>
<thead>
<tr>
<th>ASSET</th>
<th>ASSET VALUE</th>
<th>Threat description</th>
<th>Threat value</th>
<th>Control description</th>
<th>Control value</th>
<th>Total Risk Value</th>
<th>Residual</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Servers</td>
<td>GB 10</td>
<td>Unintentional Unable To Access. Accidental Loss/Damage. System/Service Failure.</td>
<td>3</td>
<td>Firewall, Network access controls. Physical security 24/7. Segregation of responsibilities and control of administrator privileges.</td>
<td>1.5</td>
<td>45</td>
<td></td>
</tr>
<tr>
<td></td>
<td>GB 10</td>
<td>Intentional Malicious Damage/Fraud. Theft (Internal/External) Unauthorised Access DDoS</td>
<td>4</td>
<td>Firewall, Network access controls. Physical security 24/7. Segregation of responsibilities and control of administrator privileges.</td>
<td>1.5</td>
<td>60</td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td>GB</td>
<td>Loss of access to email, internally and externally including sent/received documents</td>
<td></td>
<td>Back-ups and procedures. Email policy. Physical security 24/7. Segregation of responsibilities and control of administrator privileges.</td>
<td>2</td>
<td>54</td>
<td></td>
</tr>
<tr>
<td></td>
<td>GB 9</td>
<td>Unintentional Unable To Access. Accidental Loss/Damage. System/Service Failure.</td>
<td>3</td>
<td>Anti-spyware, content filtering, Anti-virus. Email Policy, Firewall. Physical security 24/7. Segregation of responsibilities and control of administrator privileges.</td>
<td>2</td>
<td>54</td>
<td></td>
</tr>
<tr>
<td>Database Server</td>
<td>GB 10</td>
<td>Loss of access to reporting tools</td>
<td></td>
<td>Back-ups, firewall, Anti-virus, Anti-spyware, security groups, group policies. Segregation of responsibilities and control of administrator privileges.</td>
<td>0.75</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>Electronic Document Storage</td>
<td>GB</td>
<td>Loss of current and historical documents, including (but not limited to) electronic copies of letters, manuals, review documents, proposals, contracts.</td>
<td></td>
<td>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.</td>
<td>0.75</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>File server</td>
<td>GB 10</td>
<td>Loss of current and historical documents, including (but not limited to) electronic copies of letters, manuals, review documents, proposals, contracts.</td>
<td></td>
<td>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.</td>
<td>1.5</td>
<td>45</td>
<td></td>
</tr>
<tr>
<td>Dropbox</td>
<td>GB 10</td>
<td>Loss of current and historical documents, including (but not limited to) electronic copies of letters, manuals, review documents, proposals, contracts.</td>
<td></td>
<td>Back-ups, firewall, Anti-virus, Anti-spyware, security groups, group policies. Physical security 24/7. Segregation of responsibilities and control of administrator privileges.</td>
<td>1.5</td>
<td>45</td>
<td></td>
</tr>
<tr>
<td>ASSET</td>
<td>RESPONSIBILITY</td>
<td>ASSET VALUE</td>
<td>Threat description</td>
<td>Threat value</td>
<td>Control description</td>
<td>Control value</td>
<td>Total Risk Value</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>----------------</td>
<td>-------------</td>
<td>------------------------------------------------------------------------------------</td>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>--------------</td>
<td>------------------</td>
</tr>
<tr>
<td>GB</td>
<td>GB</td>
<td>8</td>
<td>Unintentional Unable To Access. Accidental Loss/Damage. System/Service Failure.</td>
<td>5</td>
<td>Back-ups, Anti-virus, Anti-spyware. No document management system to improve accessibility, retrieval of docs and accidental loss.</td>
<td>2</td>
<td>80</td>
</tr>
<tr>
<td>Intranet/CRM/Helpdesk/IT Support Tools</td>
<td>GB</td>
<td>5</td>
<td>Unintentional Unable To Access. Accidental Loss/Damage. System/Service Failure.</td>
<td>3</td>
<td>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 within the application.</td>
<td>3</td>
<td>45</td>
</tr>
<tr>
<td>GB</td>
<td>GB</td>
<td>5</td>
<td>Intentional Malicious Damage/Fraud. Theft (Internal/External) Unauthorised Access DDS</td>
<td>3</td>
<td>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 within the application.</td>
<td>3</td>
<td>45</td>
</tr>
<tr>
<td>Other Electronic Data Sources</td>
<td>GB</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>GB</td>
<td>10</td>
<td>Intentional Malicious Damage/Fraud. Theft (Internal/External) Unauthorised Access</td>
<td>2</td>
<td>Secure network access (ACS), Segregation of duties for network equipment, limited/controlled access, physical security.</td>
<td>2</td>
<td>40</td>
</tr>
<tr>
<td>GB</td>
<td>GB</td>
<td>10</td>
<td>Unintentional Unable To Access. Accidental Loss/Damage. System/Service Failure.</td>
<td>4</td>
<td>Secure network access (ACS), Segregation of duties for network equipment, limited/controlled access, physical security. Resilience i.e. Duplication/repllication/redundancy</td>
<td>2</td>
<td>80</td>
</tr>
<tr>
<td>Internet (ISP)</td>
<td>GB</td>
<td>10</td>
<td>Loss of access to external network, including (but not limited to) internet, online bookings, email</td>
<td>4</td>
<td>Multiple ISP connections with automatic failover if one fails.</td>
<td>2</td>
<td>80</td>
</tr>
<tr>
<td>GB</td>
<td>GB</td>
<td>10</td>
<td>Unintentional Unable To Access. Accidental Loss/Damage. System/Service Failure.</td>
<td>4</td>
<td>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</td>
<td>1.75</td>
<td>52.5</td>
</tr>
<tr>
<td>Backup Components</td>
<td>GB</td>
<td>9</td>
<td>Intentional Malicious Damage/Fraud. Theft (Internal/External) Unauthorised Access</td>
<td>2</td>
<td>Back up processes and procedures, checklist, off site storage, physical controls, test processes.</td>
<td>2</td>
<td>36</td>
</tr>
<tr>
<td>GB</td>
<td>GB</td>
<td>9</td>
<td>Unintentional Unable To Access. Accidental Loss/Damage. System/Service Failure.</td>
<td>2</td>
<td>Back up processes and procedures, checklist, off site storage, physical controls, test processes.</td>
<td>2</td>
<td>36</td>
</tr>
</tbody>
</table>

Software Assets: application software, system software, development tools & utilities, e-Learning assets, network tools & utilities
<table>
<thead>
<tr>
<th>ASSET</th>
<th>RESPONSIBILITY</th>
<th>ASSET VALUE</th>
<th>Threat description</th>
<th>Threat value</th>
<th>Control description</th>
<th>Control value</th>
<th>Total Risk Value</th>
<th>Residual</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating Systems</td>
<td>GB</td>
<td>9</td>
<td>Intentional Malicious Damage/Fraud. Theft (Internal/External) Unauthorized Access</td>
<td>2</td>
<td>Back-ups, firewall, Anti-virus, Anti-spyware, security groups, group policies. Record assets with all the relevant info about the asset. Physical security controls.</td>
<td>2</td>
<td>36</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Unintentional Unable To Access. Accidental Loss/Damage. System/Service Failure.</td>
<td>3</td>
<td>Back-ups, firewall, Anti-virus, Anti-spyware, security groups, group policies. Record assets with all the relevant info about the asset. Physical security controls.</td>
<td>2</td>
<td>54</td>
<td></td>
</tr>
<tr>
<td>Finance System</td>
<td>GB / DB</td>
<td>Loss of access to financial system for generating invoices and purchase orders</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Back-ups, firewall, Anti-virus, Anti-spyware, security groups, group policies. Record assets with all the relevant info about the asset. Physical security controls.</td>
<td>2</td>
<td>36</td>
<td></td>
</tr>
<tr>
<td>General Productivity Tools: MS Office, Word, Excel, PowerPoint, Outlook</td>
<td>GB</td>
<td>Impact on all areas of business</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Licensing, physical and logical security measures, lack of controls of password management of the tools.</td>
<td>2</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>Phone system</td>
<td>GB</td>
<td>Loss of inbound and outbound telephone calls</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Physical security 24/7. Divert to mobile.</td>
<td>2</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>IT Development Tools -Code editors, compilers, ide environments</td>
<td>GB</td>
<td>Loss of core development tools - impacting ability to provide continued development, maintenance and support for business</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>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 within the application.</td>
<td>3</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td>ASSET</td>
<td>RESPONSIBILITY</td>
<td>ASSET VALUE</td>
<td>Threat description</td>
<td>Threat value</td>
<td>Control description</td>
<td>Control value</td>
<td>Total Risk Value</td>
<td>Residual</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------</td>
<td>-------------</td>
<td>------------------------------------------------------------------------------------</td>
<td>--------------</td>
<td>--------------------------------------------------------------------------------------</td>
<td>--------------</td>
<td>------------------</td>
<td>----------</td>
</tr>
<tr>
<td>GB</td>
<td>2</td>
<td>Unintentional</td>
<td>Unable To Access. Accidental Loss/Damage. System/Service Failure.</td>
<td>3</td>
<td>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 within the application.</td>
<td>3</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td>GB</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detailed Asset Register Listing available</td>
<td>GB</td>
<td></td>
<td>Loss of IT infrastructure, services and associated data.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Servers</td>
<td>GB</td>
<td>10</td>
<td>Intentional Malicious Damage/Fraud. Theft (Internal/External) Unauthorised Access</td>
<td>3</td>
<td>Physically Secured data centre. swipecard entry restricted to designated IT employees only. 24x7 monitoring.</td>
<td>2</td>
<td>60</td>
<td></td>
</tr>
<tr>
<td>GB</td>
<td>10</td>
<td>Unintentional</td>
<td>Unable To Access. Accidental Loss/Damage. System/Service Failure.</td>
<td>3</td>
<td>Physically Secured data centre. swipecard entry restricted to designated IT employees only. 24x7 monitoring.</td>
<td>2</td>
<td>60</td>
<td></td>
</tr>
<tr>
<td>PC's</td>
<td>GB</td>
<td>7</td>
<td>Intentional Malicious Damage/Fraud. Theft (Internal/External) Unauthorised Access</td>
<td>3</td>
<td>All PC's recorded in Asset Register. Secure building access policy.</td>
<td>2</td>
<td>42</td>
<td></td>
</tr>
<tr>
<td>GB</td>
<td>7</td>
<td>Unintentional</td>
<td>Unable To Access. Accidental Loss/Damage. System/Service Failure.</td>
<td>3</td>
<td>Acceptable use of IT policy and procedures Issues raised with the Service Desk. Under warranty.</td>
<td>3</td>
<td>63</td>
<td></td>
</tr>
<tr>
<td>Laptop's/Portable computing devices</td>
<td>GB</td>
<td>7</td>
<td>Intentional Malicious Damage/Fraud. Theft (Internal/External) Unauthorised Access</td>
<td>3</td>
<td>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.</td>
<td>4</td>
<td>84</td>
<td></td>
</tr>
<tr>
<td>GB</td>
<td>7</td>
<td>Unintentional</td>
<td>Unable To Access. Accidental Loss/Damage. System/Service Failure.</td>
<td>3</td>
<td>Remote access and Dropbox for backing up critical data to network. Insurance for lost/stolen laptops. Under warranty.</td>
<td>3</td>
<td>63</td>
<td></td>
</tr>
<tr>
<td>Monitors</td>
<td>GB</td>
<td>3</td>
<td>Intentional Malicious Damage/Fraud. Theft (Internal/External) Unauthorised Access</td>
<td>3</td>
<td>All monitors recorded in Asset Register. Secure building access policy.</td>
<td>3</td>
<td>27</td>
<td></td>
</tr>
<tr>
<td>GB</td>
<td>3</td>
<td>Unintentional</td>
<td>Unable To Access. Accidental Loss/Damage. System/Service Failure.</td>
<td>3</td>
<td>Acceptable use of IT policy. Warranty and insurance.</td>
<td>2</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td>Printers / Scanner</td>
<td>GB</td>
<td>3</td>
<td>Intentional Malicious Damage/Fraud. Theft (Internal/External) Unauthorised Access</td>
<td>3</td>
<td>All printers recorded in Asset Register. Standard printers utilised for ease of maintenance/replacement/support. Physical building policy. 24x7 monitoring.</td>
<td>3</td>
<td>27</td>
<td></td>
</tr>
<tr>
<td>GB</td>
<td>3</td>
<td>Unintentional</td>
<td>Unable To Access. Accidental Loss/Damage. System/Service Failure.</td>
<td>3</td>
<td>Internal IT Support with full hardware maintenance contract. Standard printers utilised thoughout for easy maintenance/replacement. 24x7 monitoring.</td>
<td>3</td>
<td>27</td>
<td></td>
</tr>
<tr>
<td>Routers &amp; Switches &amp; Firewalls</td>
<td>GB</td>
<td>10</td>
<td>Intentional Malicious Damage/Fraud. Theft (Internal/External) Unauthorised Access</td>
<td>3</td>
<td>Physically Secured data centre swipe card entry restricted to designated IT employees only. Fully monitored via Munin Monitoring system.</td>
<td>3</td>
<td>90</td>
<td></td>
</tr>
<tr>
<td>ASSET</td>
<td>RESPONSIBILITY</td>
<td>ASSET VALUE</td>
<td>Threat description</td>
<td>Threat value</td>
<td>Control description</td>
<td>Control value</td>
<td>Total Risk Value</td>
<td>Residual</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------</td>
<td>-------------</td>
<td>--------------------------------------------------------</td>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>---------------</td>
<td>-----------------</td>
<td>----------</td>
</tr>
<tr>
<td>GB</td>
<td>GB</td>
<td>10</td>
<td>Unintentional. Unable To Access.</td>
<td>3</td>
<td>Physically Secured data centre swipe card entry restricted to designated IT employees only. Fully monitored via Munin Monitoring system.</td>
<td>2</td>
<td>60</td>
<td></td>
</tr>
<tr>
<td>GB</td>
<td>GB</td>
<td>3</td>
<td>Intentional. Malicious Damage/Fraud. Theft (Internal/External) Unauthorized Access</td>
<td>3</td>
<td>All phones recorded in the Asset Register. Physical building policy.</td>
<td>3</td>
<td>27</td>
<td></td>
</tr>
<tr>
<td>GB</td>
<td>GB</td>
<td>3</td>
<td>Unintentional. Unable To Access.</td>
<td>3</td>
<td>All phones recorded in the Asset Register. Physical building policy.</td>
<td>3</td>
<td>27</td>
<td></td>
</tr>
<tr>
<td>Mobile phones</td>
<td>GB</td>
<td>3</td>
<td>Intentional. Malicious Damage/Fraud. Theft (Internal/External) Unauthorized Access</td>
<td>4</td>
<td>All phones recorded in Asset Register. Password protected. Ease of replacement. Centrally managed with ability to lock/wipe phone if lost/stolen.</td>
<td>3</td>
<td>36</td>
<td></td>
</tr>
<tr>
<td>GB</td>
<td>GB</td>
<td>3</td>
<td>Unintentional. Unable To Access.</td>
<td>4</td>
<td>All phones recorded in Asset Register. Password protected. Ease of replacement. Centrally managed with ability to lock/wipe phone if lost/stolen.</td>
<td>4</td>
<td>48</td>
<td></td>
</tr>
<tr>
<td>USB devices</td>
<td>GB</td>
<td>5</td>
<td>Intentional. Malicious Damage/Fraud. Theft (Internal/External) Unauthorized Access</td>
<td>4</td>
<td>Encryption used where required. Removable Media Policy</td>
<td>3</td>
<td>60</td>
<td></td>
</tr>
<tr>
<td>GB</td>
<td>GB</td>
<td>5</td>
<td>Unintentional. Unable To Access.</td>
<td>5</td>
<td>Removable Media Policy</td>
<td>3</td>
<td>75</td>
<td></td>
</tr>
<tr>
<td>UPS</td>
<td>GB</td>
<td>7</td>
<td>Intentional. Malicious Damage/Fraud. Theft (Internal/External) Unauthorized Access</td>
<td>3</td>
<td>Located in secure Computer room (IT Staff Only). UPS devices monitored by IT Team. Data centre UPS features redundancy and backup diesel generators</td>
<td>2.5</td>
<td>52.5</td>
<td></td>
</tr>
<tr>
<td>GB</td>
<td>GB</td>
<td>7</td>
<td>Unintentional. Unable To Access.</td>
<td>3</td>
<td>Dual power supply to Computer room - load balancing of key servers/devices.</td>
<td>2.5</td>
<td>52.5</td>
<td></td>
</tr>
<tr>
<td>GB</td>
<td>GB</td>
<td>7</td>
<td>Unintentional. Unable To Access.</td>
<td>3</td>
<td>For GRDC data centre, SLA in place with colocation provider for provision of HVAC environment.</td>
<td>3</td>
<td>63</td>
<td></td>
</tr>
</tbody>
</table>

Environmental
<table>
<thead>
<tr>
<th>ASSET</th>
<th>RESPONSIBILITY</th>
<th>ASSET VALUE</th>
<th>Threat description</th>
<th>Threat value</th>
<th>Control description</th>
<th>Control value</th>
<th>Total Risk Value</th>
<th>Residual</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property/building</td>
<td>GB</td>
<td>8</td>
<td>Intentional/Unintentional</td>
<td>4</td>
<td>Multi-tenanted occupancy, covering 1st floor. Floor plans available. The buildings and contents are insured. H &amp; 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 security breach should be raised with GB. If unable to access the buildings then back-ups are in place. Capability exists to support remote working.</td>
<td>2</td>
<td>64</td>
<td></td>
</tr>
<tr>
<td>Desks/seating for staff/visitors</td>
<td>GB</td>
<td>2</td>
<td>Intentional/Unintentional</td>
<td>2</td>
<td>Desks and seating for staff where possible are located to maximise space and privacy</td>
<td>4</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>Air-Conditioning</td>
<td>GB</td>
<td>5</td>
<td>Intentional/Unintentional</td>
<td>5</td>
<td>Air conditioning units vent to be kept clear of paperwork/clutter to prevent malfunction. AC units tested regularly. There is an AC unit in the Server room which has been tested and is regularly maintained.</td>
<td>2</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>Stationary inc. calculators Desk fans</td>
<td>GB</td>
<td>1</td>
<td>Intentional/Unintentional</td>
<td>3</td>
<td>Secure 24/7 environment</td>
<td>4</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>Photo-copiars/fax machines</td>
<td>GB</td>
<td>2</td>
<td>Intentional/Unintentional</td>
<td>3</td>
<td>Secure 24/7 environment</td>
<td>4</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td>Shredder</td>
<td>GB</td>
<td>2</td>
<td>Intentional/Unintentional</td>
<td>3</td>
<td>Secure 24/7 environment</td>
<td>4</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td>Reputation</td>
<td>BC</td>
<td>8</td>
<td>Unintentional/Intentional</td>
<td>3</td>
<td>Brand guidelines, controls over intranet and internet. Guidelines created for staff. Maintain links with industry journalists. Designated spokespersons to respond to press enquiries.</td>
<td>3</td>
<td>72</td>
<td></td>
</tr>
<tr>
<td>Brand</td>
<td>BC</td>
<td>8</td>
<td>Unintentional/Intentional</td>
<td>3</td>
<td>Brand guidelines, controls over intranet and internet. Guidelines created for staff. Maintain links with industry journalists. Designated spokespersons to respond to press enquiries.</td>
<td>3</td>
<td>72</td>
<td></td>
</tr>
<tr>
<td>Service</td>
<td>BC</td>
<td>8</td>
<td>Unintentional/Intentional</td>
<td>3</td>
<td>Brand guidelines, controls over intranet and internet. Guidelines created for staff. Maintain links with industry journalists. Designated spokespersons to respond to press enquiries.</td>
<td>3</td>
<td>72</td>
<td></td>
</tr>
</tbody>
</table>

Physical Documents & Information Sources
<table>
<thead>
<tr>
<th>ASSET</th>
<th>RESPONSIBILITY</th>
<th>ASSET VALUE</th>
<th>Threat description</th>
<th>Threat value</th>
<th>Control description</th>
<th>Control value</th>
<th>Total Risk Value</th>
<th>Residual</th>
</tr>
</thead>
<tbody>
<tr>
<td>Marketing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unpublished marketing data</td>
<td>LL</td>
<td>5</td>
<td>Intentional Malicious Damage/Fraud. Theft (Internal/External) Unauthorised Access</td>
<td>2</td>
<td>Internal marketing team is responsible for release of material to PR agencies. Material is stored in Dropbox and source code repository</td>
<td>3</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td>Press releases, marketing literature, references, presentation, client/sovereign logo's</td>
<td>LL</td>
<td>7</td>
<td>Unintentional Unable To Access. Accidental Loss/Damage. System/Service Failure.</td>
<td>2</td>
<td>IT controls - data backed up. Info transferred by email. Clear instructions on the approval process.</td>
<td>3</td>
<td>42</td>
<td></td>
</tr>
<tr>
<td>supplier contracts</td>
<td>LL</td>
<td>5</td>
<td>Intentional/Unintentional Malicious Damage/Fraud. Theft (Internal/External) Unauthorised Access</td>
<td>2</td>
<td>Stored in Excel IT Supplier list spreadsheet in Dropbox</td>
<td>7</td>
<td>70</td>
<td></td>
</tr>
<tr>
<td>Website/intranet content</td>
<td>LL</td>
<td>8</td>
<td>Intentional Malicious Damage/Fraud. Theft (Internal/External) Unauthorised Access</td>
<td>3</td>
<td>Content is managed via revision control and hosted securely. An online CMS is &quot;not&quot; used so modification is not easy. All web content is encrypted and internal data is protected by username and password</td>
<td>2</td>
<td>48</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LL</td>
<td>8</td>
<td>Unintentional Unable To Access. Accidental Loss/Damage. System/Service Failure.</td>
<td>2</td>
<td>Approval process to prevent misuse</td>
<td>3</td>
<td>48</td>
<td></td>
</tr>
<tr>
<td>Budgets</td>
<td>BC/DB</td>
<td>6</td>
<td>Unintentional Unable To Access. Accidental Loss/Damage. System/Service Failure.</td>
<td>4</td>
<td>Managed by BC and DB and approval given to selected staff members</td>
<td>2</td>
<td>48</td>
<td></td>
</tr>
<tr>
<td>Business Development</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proposals</td>
<td>BC</td>
<td>5</td>
<td>Intentional Malicious Damage/Fraud. Theft (Internal/External) Unauthorised Access</td>
<td>2</td>
<td>Documents stored on Dropbox that is shared by internal 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.</td>
<td>2</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td></td>
<td>BC</td>
<td>5</td>
<td>Unintentional Unable To Access. Accidental Loss/Damage. System/Service Failure.</td>
<td>4</td>
<td>As above. Review of proposal and sign off before distribution to clients. Proposals marked as commercial in confidence.</td>
<td>2</td>
<td>40</td>
<td></td>
</tr>
<tr>
<td>Performance reports (SLA)</td>
<td>GB</td>
<td>2</td>
<td>Intentional Malicious Damage/Fraud. Theft (Internal/External) Unauthorised Access</td>
<td>2</td>
<td>Certain SLA reports are published publically. Internal reports are held inside monitoring systems on the intranet</td>
<td>3</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>ASSET</td>
<td>RESPONSIBILITY</td>
<td>ASSET VALUE</td>
<td>Threat description</td>
<td>Threat value</td>
<td>Control description</td>
<td>Control value</td>
<td>Total Risk Value</td>
<td>Residual</td>
</tr>
<tr>
<td>-------</td>
<td>----------------</td>
<td>-------------</td>
<td>-------------------</td>
<td>--------------</td>
<td>---------------------</td>
<td>---------------</td>
<td>-----------------</td>
<td>----------</td>
</tr>
<tr>
<td>HR</td>
<td>GB</td>
<td>2</td>
<td>Unintentional</td>
<td>2</td>
<td>As above</td>
<td>3</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Unintentional</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Unable To Access.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Accidental Loss/Damage.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>System/Service Failure.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Malicious damage/fraud. Theft. Willful damage.</td>
<td></td>
<td>Locked filing cabinets. JW has access.</td>
<td>3</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td></td>
<td>JW</td>
<td>2</td>
<td>Unable to access</td>
<td>4</td>
<td>Soft copies available - restricted access.</td>
<td>3</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td></td>
<td>JW</td>
<td>2</td>
<td>Accidental loss/damage. Disclosure of information. Breach of legislation i.e. Data protection Act.</td>
<td>4</td>
<td>Soft copies available - restricted access.</td>
<td>2</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td></td>
<td>JW</td>
<td>2</td>
<td>Unauthorised access.</td>
<td>4</td>
<td>Information Security controls.</td>
<td>3</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td></td>
<td>JW</td>
<td>8</td>
<td>Malicious damage/fraud/Theft</td>
<td>4</td>
<td>Information is held at our accountants in addition to JW</td>
<td>2</td>
<td>64</td>
<td></td>
</tr>
<tr>
<td>Finance</td>
<td>DB</td>
<td>7</td>
<td>Intentional</td>
<td>4</td>
<td>Locked filing cabinets. Physical security of the building. Electronic records are backed up. Access to registry financial reports is controlled.</td>
<td>2</td>
<td>56</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DB</td>
<td>7</td>
<td>Malicious Damage/Fraud. Theft (Internal/External) Unauthorised Access</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Misc</td>
<td>IST</td>
<td>4</td>
<td>Intentional/Unintentional</td>
<td>3</td>
<td>Copies are held in Dropbox and so are distributed among IST members.</td>
<td>4</td>
<td>48</td>
<td></td>
</tr>
<tr>
<td></td>
<td>JW</td>
<td>2</td>
<td>Intentional/Unintentional</td>
<td>4</td>
<td>Office manned during office hours and locked otherwise. Completed pages are archived in a locked filing cabinet.</td>
<td>4</td>
<td>32</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IST</td>
<td>4</td>
<td>Intentional/Unintentional</td>
<td>3</td>
<td>Copies are held in Dropbox and so are distributed among IST members. Hard copies distributed to IST members to keep at home.</td>
<td>4</td>
<td>48</td>
<td></td>
</tr>
<tr>
<td></td>
<td>GB</td>
<td>3</td>
<td>Intentional/Unintentional</td>
<td>4</td>
<td>Agreements are controlled via designated managers</td>
<td>4</td>
<td>48</td>
<td></td>
</tr>
<tr>
<td></td>
<td>JW</td>
<td>1</td>
<td>Intentional/Unintentional</td>
<td>1</td>
<td>Reception manages the subscriptions</td>
<td>7</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DB</td>
<td>7</td>
<td>Intentional</td>
<td>3</td>
<td>Locked filing cabinets.</td>
<td>2</td>
<td>42</td>
<td></td>
</tr>
<tr>
<td>ASSET</td>
<td>RESPONSIBILITY</td>
<td>ASSET VALUE</td>
<td>Threat description</td>
<td>Threat value</td>
<td>Control description</td>
<td>Control value</td>
<td>Total Risk Value</td>
<td>Residual</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>----------------</td>
<td>-------------</td>
<td>-----------------------------------------------</td>
<td>--------------</td>
<td>--------------------------------------------------------------------------------------</td>
<td>---------------</td>
<td>-----------------</td>
<td>----------</td>
</tr>
<tr>
<td>DropBox</td>
<td>GB</td>
<td>7</td>
<td>Intentional Malicious Damage/Fraud. Theft (Internal/External) Unauthorized Access</td>
<td>5</td>
<td>Dropbox provides version control and restoration from backups. Files are stored on each person's computers and &quot;in the cloud.&quot; Files on the Dropbox website are protected by a username and password.</td>
<td></td>
<td>2</td>
<td>70</td>
</tr>
<tr>
<td>Cryptographic Material &amp; Credentials</td>
<td>GB</td>
<td>8</td>
<td>Intentional Malicious Damage/Fraud. Theft (Internal/External) Unauthorized Access</td>
<td>6</td>
<td>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</td>
<td></td>
<td>2</td>
<td>96</td>
</tr>
<tr>
<td>Petty Cash</td>
<td>JW</td>
<td>7</td>
<td>Intentional Malicious Damage/Fraud. Theft (Internal/External) Unauthorized Access</td>
<td>5</td>
<td>Locked filing cabinet.</td>
<td></td>
<td>2</td>
<td>70</td>
</tr>
<tr>
<td>Business Systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shared Registry System</td>
<td>GB</td>
<td>10</td>
<td>Intentional/Accidental ACCIDENTAL LOSS/DAMAGE UNAUTHORISED ACCESS SYSTEM/SERVICE FAILURE</td>
<td>6</td>
<td>Physical security of server, firewalls, access control, logging/monitoring, resilience to hardware/network failure</td>
<td></td>
<td>1</td>
<td>60</td>
</tr>
<tr>
<td>Whois Service</td>
<td>GB</td>
<td>10</td>
<td>Intentional Malicious Damage/Fraud. Theft (Internal/External) Unauthorized Access</td>
<td>7</td>
<td>Physical security of server, firewalls, access control, logging/monitoring, resilience to hardware/network failure. Rate limiting (abuse preventative measures).</td>
<td></td>
<td>1</td>
<td>70</td>
</tr>
<tr>
<td>Authoritative DNS Service</td>
<td>GB</td>
<td>10</td>
<td>Intentional Malicious Damage/Fraud. Theft (Internal/External) Unauthorized Access</td>
<td>10</td>
<td>Physical security of server, firewalls, access control, logging/monitoring, resilience to hardware/network failure. Overprovisioning to withstand DDoS attacks. Use of Tsig (transaction signature) and VPN to prevent tampering of zone data. Use of anycast to provide load balancing and isolation of attacks.</td>
<td></td>
<td>1</td>
<td>100</td>
</tr>
<tr>
<td>DNSsec signing system</td>
<td>GB</td>
<td>10</td>
<td>Intentional Malicious Damage/Fraud. Theft (Internal/External) Unauthorized Access</td>
<td>5</td>
<td>Physical security of server, firewalls, access control, logging/monitoring, resilience to hardware/network failure. Securing of cryptographic material (keys).</td>
<td></td>
<td>1</td>
<td>50</td>
</tr>
<tr>
<td>Zone File Access System</td>
<td>GB</td>
<td>10</td>
<td>Intentional Malicious Damage/Fraud. Theft (Internal/External) Unauthorized Access</td>
<td>3</td>
<td>Physical security of server, firewalls, access control, logging/monitoring, resilience to hardware/network failure</td>
<td></td>
<td>1</td>
<td>30</td>
</tr>
</tbody>
</table>