|  |
| --- |
| **Question** |
| Your organisation has established a process to identify, assess and manage information security risks. |
| Senior management have approved and published an appropriate information security policy. |
| Your organisation has established written agreements with third party service providers that include appropriate information security conditions. |
| Your organisation ensures the management of data security breaches, including communication of information security events and weaknesses. |
| Your organisation has established regular information security awareness training for all staff. |
| Your organisation ensures that employees and contractors are aware of and fulfil their information security responsibilities. |
| Your organisation has established entry controls to restrict access to premises and equipment on a need-to-know basis. |
| Your organisation prevents un-authorised physical access, damage and interference to personal data. |
| Your organisation has established a process to securely dispose of records and equipment when no longer required. |
| Your organisation has established a mobile working policy which includes the use of mobile computing devices and removable media |
| Your organisation has established effective anti-malware defences to protect computers from malware infection. |
| Your organisation has established a process to routinely back-up electronic information to help restore information in the event of disaster. |
| Your organisation has established a process to ensure software is kept up-to-date and the latest security patches are applied. |
| Your organisation is aware of customer rights under Data Protection legislation, and can comply. |