PERRY JOHNSON REGISTRARS, INC.

Key Components of ISO 27001

ISO 27001 isn't an appliance or piece of software that guarantees data breaches won't happen, because such a thing doesn't exist, it requires adherence to an internationally formalized standard where your company is required to write and implement procedures based on the actual written standard. Education, awareness, formalized processes, continual review and improvement, and commitment from all members of an organization are the keys to an effective ISMS. The number of exploits and vulnerabilities in electronic systems and software are so great that it is difficult to rely on a piece of software or hardware and believe that your information security is taken care of.

- Only internationally recognized and accredited information security management standard that is able to be certified by third parties. The best option to advertise commitment and achievement of organizational information security systems to customers. Rapidly being required by many organizations to even be allowed to bid on contracts.

- People are the most important part of information security, ISO 27001 requires security awareness for individuals who affect information security and provides the framework for instituting a culture of making information security a top priority. Employees will always be the weakest link in information security, it's extremely difficult to prevent them from giving the sensitive data you want to protect away as they don't need to carry it out of the building with them in a big box. A breach could be as innocent as a casual conversation after work out with friends; overheard by the wrong person.

- Cyber Security threats evolve and change at an incredible rate, new vulnerabilities are typically identified because they have been employed to breach security. Having a formalized response plan in place for a breach as ISO 27001 requires will greatly reduce the damage and duration caused by an attack. Failing to plan is planning to fail.

- After implementing your ISMS (information Security management system) to ISO 27001 guidelines you will know and prioritize what your biggest threats are based on the damage potential to the company including financial, legal, contractual, reputation, or any factors which you determine are material to your company. This information will be communicated and reviewed to top management at all relevant levels on an ongoing basis so that the necessary resources and actions can be put into place to control any levels of risk that are higher then you are willing to accept. Ignorance does not excuse responsibility in a court of law, or public opinion.

BENEFITS:

- Top management can leverage the certification in order to gain new business. Achieving ISO 27001 certification will put your company on the radar to gain business from sectors where information security is critical and assurance of protection of the information assets viewed and handled while the work is being carried is required by the organization taking bids. Being able to advertise certification to an internationally recognized standard in information security will make you more attractive to potential customers and stakeholders.