ISMS Primer

- What is an ISMS

ARTICLES

Why an ISMS ?

Any IT Division or Department is managed with different processes, technology and People; this is called an ”Information Management System” and is for the most part done manually with Word and Excel.

An Information Security Management System (ISMS) is a systematic approach to managing these domains in order to ensure the confidential or sensitive company information remains secure. It is what is being done today; in a structured way with a focus on Information Security.

For additional information please see : https://advisera.com/27001academy/what-is-iso-27001/

Which Standards support this approach?

There are many standards supporting the management of IT; eg. ITIL, COBIT, NIST, ISMS and many more.
From an Information Security Management point of view, most certification bodies recommend aligning your ISMS to ISO 27001, the internationally recognised information security standard.

How long does it take to implement an ISMS ?

For a mid-sized organisation having a focussed project utilising the enablement systems in use today, a typical ISMS implementation could be achieved in 4 to 8 months. This is then followed up with imbedding the implemented processes over a few months before certification can be explored.

In most cases a Spotica implementation is done at a fraction (20-30%) of this time and cost.

Challenges experienced when implementing an ISMS.

One of the biggest challenges companies face when they implement an ISMS is the mammoth task of translating the standard into company specific actions and processes. This is closely followed by performing the risk assessment and trying to identify the Scope of the ISMS. Not to mention the creation of the documentation which in itself can take up to 12 months to review/translate and create all the required policies and procedures.

Spotica did the hard yards and all of this comes out of the box. Automatically being customised during the implementation and immediately ready to use.

Who requires an ISMS ?

Every company that has an IT Capability and manages client or private data needs to ensure the confidentiality of the data. This is especially imperative for all listed and regulated companies.

Do I have to become ISO certified ?

Not necessarily. Through implementing the guidelines as given from ISO 27001 into the way the business is being managed creates a structured method of securely managing the IT operations.

Certification is usually done for external stakeholder affirmation but not a necessity for managing the environment according to ISO 27001 principles.

Spotica and Certification

Spotica is foremost designed around advising your specific business on what to do and how you're fairing to secure your confidential and private data.

It is build on ISO 27001 and other industry standards and paves the way for certification while in it's core it is designed to guide you on what to do to protect your data.

Therefore various options exists:

- Implement the system as-is to secure your data
- If you already have an ISMS today, digitize what you have and make it amazingly simple
- Run a full ISMS certification project from scratch and use Spotica as the bases thereof