What is an ISMS and why do you need one?

An Information Security Management System (ISMS) is a systematic approach using processes, technology and people that helps you protect and manage your organisation's information through risk management.

An ISMS helps your organisation by:

- Securing your information
- Increasing your resilience to attacks
- Reducing costs associated with information security:
- Protect the confidentiality, availability and integrity of your data

What is included in an ISMS?

An ISMS contains:

- A catalogue of what information and business assets used to store and interact with the information you are looking to protect.
- Policies that define behaviour staff are expected to demonstrate when working for your organisation.
- Procedures and actions for monitoring and protecting your organisations information assets.
- What technology is used and its configuration.

Where do I start?

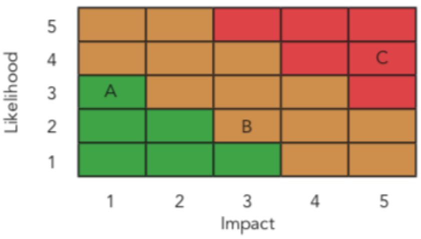
1. ### Understand the terms
   The first step is to understand some of the common terms used in an ISMS, such as "Risk", "Impact", "likelihood", "Controls", "threats", "vulnerabilities", "ISO27001".

2. ### Establish a risk assessment framework
   A risk framework defines the organisation's top-level needs and obligations, and the organisation's attitude to risk. These key elements will influence how the rest of the risk assessment is conducted.

3. ### Identify risks
   The first step of risk identification is to develop an asset register for the organisation's information assets. These assets will dictate the types of risks your organisation faces, and includes hardware, information stores, people and physical locations.

4. ### Analyse risks
   For each risk you identify, you should be able to analyse the likelihood of each threat exploiting a related vulnerability and the harm that threat can cause.

The risk analysis and evaluation are often presented in terms of a simple chart or matrix that combines likelihood and impact, and is colour-coded to identify acceptable risk, moderate risk and unacceptable risk. See insert.



5. Evaluate risks
   Once you have analysed your risks, you need to evaluate them against your risk acceptance criteria. Only once you have done this can you decide the appropriate way to mitigate each risk and the priorities for doing so.

6. Mitigate these risks
   Once you have determined which risks must be mitigated, there are four common recognised method to manage your risks:

   - Modify the risk, normally by applying security controls that will reduce likelihood and/or impact. This is the most common approach.
   - Accept the risk – accept that it falls within previously established risk acceptance criteria, or via extraordinary decisions.
   - Avoid the activity or circumstance causing the risk. This is often not practical, however.
   - Share the risk with a partner such as through insurance or by outsourcing to a supplier that can better manage the risk.

How do I build an ISMS?

If you are starting from scratch, the following steps are proven to be the most successful method to building an effective ISMS.

1. Setup an official project
   You should treat the implementation of an ISMS like any normal project: you will need to ensure there is a budget for it, you have the right people engaged and you have the right level of oversight setup.

2. Setup the ISMS fundamentals
   Where will it be stored? What format will it be in? (Paper-based, or software-based) What software runs it? Who owns it?

3. Establish the scope
   These are the controls that the organisation must have in place to consider the ISMS to be operational. See our recommendations on which controls to begin with below.

4. Establish how you will manage risk
   Essentially, this comes down to: What will you do, what technology you use (if any), when you will do it (and how often), and who will do it.

For smaller organisations, it is important not to try to do everything at once. Start with implementing one control at a time. Additionally, we recommend establishing technology and FTE requirements up front; many ISMS implementations stumble when the organisation runs out of resources halfway through.

What controls should I start with?

Small businesses have some unique challenges around resources, access to technology and often do not have large funds to spend on a full-blown ISMS. However, a lightweight ISMS can be run on a very lean budget and still provide value to the organisation. With this in mind, we recommend the following controls for their “bang per buck”.

1. The assignment of responsibilities for specific tasks within the ISMS
2. Identify specific controls for the laws and regulations that apply to your organisation.
3. Human resource security
4. Performing asset management
5. Managing access control
6. Managing physical and environmental security
7. Managing Operational security
8. Managing communications security.

How much time should I allocate to managing an ISMS?

We have purposely chosen to recommend the above controls for their ease of adoption and management. We believe that – once established – these controls will require around **0.5-1.0 man days per month to operate**. If your organisation has more complex requirements or you do not have a qualified expert in-house, you may wish to consider a external provider to help you with an ISMS-as-a-service.

Conclusion

While an ISMS seems like a large undertaking, both to build and to run, much of the benefits can be obtained with a relatively small effort; it can be as little as half a day per month for the average SME. The above recommendations will help you get started on the journey towards the design and implementation of a practical ISMS. If required, LEANmade can help you setup your ISMS and the controls within.

The most important thing to remember is: get started, take small steps, and don’t try to over-design and over-complicate.