Why everyone needs to consider Information Security and ISO 27001

With the enactment of the General Data Protection Regulation (GDPR) in May 2018, the world of Information Security was shaken and changed forever. The regulation spans far and wide and changes how any organisation must process information.

Furthermore, small businesses in the UK are the target of an estimated 65,000 attempted cyber attacks every day. So with this in mind, we'll explore why Information Security is important to all organisations, and what can they do to combat this?

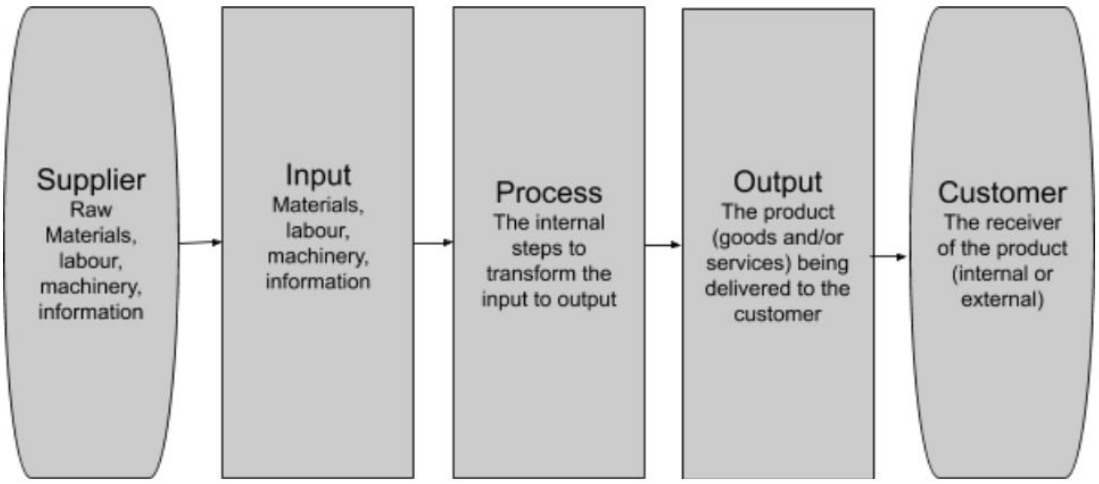
What is Information Security?

Information security often referred to as InfoSec, refers to the processes and tools designed and deployed to protect sensitive business information from modification, disruption, destruction, and inspection. The International Organisation for Standardization defines Information Security as the preservation of confidentiality, integrity and availability of information.

This is translated into an organisation ensuring that there is adequate staff training in place, contracts, supplier management, etc., to reduce the risk of information security incidents.

I'm not a Software as a Service Company, why do I need to worry about Information Security?

Ultimately, all organisations consist of inputs, processes and outputs known as IPO. Below is the Supplier, input, process, output and customer (SIPOC) example.



As you can see from the diagram, information flows throughout the entire lifecycle of any organisation, so just because you're not a software organisation does not mean you don't need information security.

To emphasise that organisations of all sizes, contexts and industries are vulnerable to Information Security incidents, we have listed some notable examples:

- In 2016, Uber reported that hackers stole the information of over 57 million riders and drivers.
- In 2018, Under Armor reported that its "My Fitness Pal" was hacked, affecting 150 million users.
- This is not only limited to large organisations, according to Hiscox one small business in the UK is successfully hacked every 19 seconds.

What type of information do I need to protect?

Now that we have established that organisations of all kinds are vulnerable to Information Security risks, we'll explore a little further the specific type of information at risk. We've broken this into 3 large categories:

1. Business Data including financial - This information relates to organisational performance metrics, documentation and financial information.

2. Employee Data - All organisations have employees of some kind, which means that they will hold sensitive employee information such as phone numbers, national insurance numbers, bank and salary details for example.
3. Intellectual Property - Many organisations are likely to have Intellectual Property that they must protect. This is an area that organisations must protect to ensure their Unique Selling Point (USP) is not compromised.

What are the risks?

The information security risks that face an organisation are great, however, we have attempted to break this into two threat categories to make it easy to digest. Information Security threats exist in two forms:

- Internal Threats - Internal threats are threats that begin within a company, government agency, or institution, normally by an unhappy employee who perhaps was informed that soon he would be out of work or would not get a promotion that he'd been hoping for. The damage or threat does not necessarily have to be done by the employee himself, but rather he may be manipulated into allowing it. Stay aware of moods and tendencies within your team.
- Examples include:
    - Stealing/leaking of information
    - Allowing external agents access to company sensitive systems or information

- External Threats - Threats coming from outside the company always entail ill intent. They are performed to steal data, disrupt company processes, and damaging the company's operation. Outside attackers often attempt to manipulate a company's personnel and appeal to an employee's good nature to take advantage. They may pose as an official company's tech support, requesting sensitive information, which may reveal the organization's weaknesses.
- Examples include:
    - Phishing
    - Hacking

How to begin protecting information?

Organisations often believe that implementing Information Security will be a daunting and expensive prospect, with high on-going costs. Assumptions are that it will require a whole new set of systems and procedures and that the system requires complex, documented, detailed procedures, forms and records.

ISO 27001 is a highly respected international standard for information security management. Whilst organisations can seek certification to the standard, it also offers a good framework to work to even without going for certification. Our recommended approach is to utilise the framework of ISO 27001 to conduct a gap analysis to assess the health of your infosec system.

An organization that wants to improve its security management system using ISO 27001 as its standard would undergo the following activities:

- Gap analysis: The first step, a gap analysis is performed either by the organization or by an outside expert. A gap analysis helps the organization understand which requirements and controls it does and doesn't comply with.
- Remediation: For any requirements and controls with which the organization is not compliant, it can make changes to its personnel (such as training), processes, and technologies to meet the requirements of the standard.

If an organisation desires to seek certification to win new business as well as protect the information security, some additional steps exist:

- External audit: An organization that needs to demonstrate compliance via an external audit can hire a competent security assessment firm to perform an audit with a detailed audit report and opinion of compliance.
- Certification and registration: An organization can choose to undergo a higher-quality external audit by employing one of the organizations authorized to certify and register an organization as ISO 27001 compliant. The advantage is that the audit firm is held to a high standard on ISO 27001 audits. ISO 27001 certification is generally more costly than an external audit but may be required in some circumstances.