Information Security Management

Do you know how to securely manage your information?

About Information Security Management

Information Security Management relates to all types of information, be it paper-based, electronic or other. It determines how information is processed, stored, transferred, archived and destroyed.

A secure information management system is one which ensures:

- confidentiality, so that only those who are authorised to see the information have access to it
- integrity, so that the accuracy and completeness of the information is safeguarded by robust sourcing, processing, updating and storage processes
- availability, so that authorised users have access to information and associated assets, in the required forms, when they need it.

Information Security Management is about the protection of information assets from potential security breaches. It starts with reviewing risks, setting policies, processes and controls, and by implementing them throughout the organisation.

A global standard for Information Security Management

Recognition of the importance of Information Security Management is now widespread. In fact, a Standard outlining the criteria of effective information management practice has been released.
The Standard: AS/NZS 7799.2:2003 – Specification for Information Security Management Systems and AS/NZS ISO/IEC 17799:2001 Information Technology – Code of Practice for Information Security Management brings our region in line with best practice information security management on a global scale.
They offer organisations a practical framework and guidelines to help improve the management of information security, and be recognised accordingly – worldwide.
Originally developed by major international industry organisations, both documents have been improved and refined to ensure widespread practical application at international levels, and AS/NZS 7799.2:2003 or BS 7799.2:2002 are the standards against which organisations can be certified.

What benefits can effective Information Security Management deliver to your business?

In addition to a system which aims to ensure confidentiality, integrity and availability, an effective information security management system provides a framework to deliver :

- clear criteria which assist your organisation in continually improving its performance
- an independent measure of how your organisation delivers its service
- increased skills, confidence and accountability amongst your staff
- a transparent review and assessment that clearly defines to all stakeholders their respective roles and responsibilities
- a professional image to customers, suppliers and Government
- recognition within your industry that industry requirements are paramount.

At the very least, failure to effectively manage information security can result in:

- loss of business through loss of critical commercial information
- vulnerability to losses through computer fraud, fire and flood
- losses through technical accident, ineptitude or malfunction
- losses through denial of service, hacking, computer viruses or other forms of industrial sabotage
- losses as a result of links with faulty or insecure systems eg. partners or suppliers.

What industries and business types will benefit?

Any business in which information is a key enabler of core business, or where extensive records are required, can benefit from improved Information Security Management.

For example:

- data centres and record storage facilities
- global security centres
- network operation centres
- e-commerce providers
- providers of secure infrastructures and system integrators
- IT-related businesses
- inhouse IT functions
- software development specialists
- public sector organisations
- defence-related industries and support agencies
- banks, insurance and related organisations
- telecommunications and healthcare organisations

Pathways to effective Information Security Management

SAI Global offers a range of options to suit the information security management needs of different types and sizes of business.
These options range from certification, with all the benefits and international recognition it brings, to a number of information security improvement or assessment alternatives, which may also act as building blocks to certification.
No matter which pathway you choose, SAI Global's assessments are planned and conducted in the context of your existing business management system, with the aim of smooth, easy integration and, to the greatest extent possible, uninterrupted business practice.

Option 1:
Certification to AS/NZS 7799 Part 2:2003 or BS 7799.2:2002

Certification to AS/NZS 7799 involves your organisation making a commitment to developing an Information Security Management system that, within a certain defined scope, meets the requirements of the Standard.
SAI Global offers expertise along the way, including assistance with defining your scope.
Once you are happy that your information security policies have been defined and implemented according to the requirements of the Standard, SAI Global's expert auditors will assess your system.
Organisations which are certified by SAI Global to AS/NZS 7799 earn the right to display the SAI Global ISMS certification mark.
This is a signal to your customers, employees and other stakeholders that your organisation has invested in a system to meet the most widely recognised international benchmark standard of Information Security Management practices.

Option 2:
Information Security Management Gap Analysis*

SAI Global's technical experts can examine your organisation's nominated Information Security Management processes, and provide you with a detailed report indicating where improvements can be made. This report can be used as the starting point for developing a more effective Information Security Management system, whether independently or through the SAI Global certification program.
There is no obligation to commit to certification, however, expert identification of areas of risk can form an important building block for developing a certified system.

Option 3:
Second party assessment against your organisation's own selected criteria*

If your organisation already has an Information Security Management system in place, SAI Global can assess its performance in practice. This will ascertain whether your own system is effectively meeting your own performance criteria – whatever that may be. This form of assessment offers your organisation and its key stakeholders objective assurance regarding the integrity of its selected information systems.

Option 4:
Second party assessments – examination of suppliers and business partners*

Modern organisations and their information systems are increasingly linked to others, for example suppliers and business partners, forming a business information chain. The chain, however, is only as strong as its weakest link.
SAI Global can assess Information Security Management practice and process performance of such related organisations, and provide a detailed account of their practical performance, including areas of potential vulnerability.
This enables your organisation to make informed decisions regarding the most appropriate partner and supplier relationships, define how they should be conducted, and protect itself against a wide range of risks. [•]

Re-printed with a permission from SAI-Global Limited. For more info e-mail to assurance@sai-global.com