Kiowa Security provides consultancy services in a range of areas of information security*, including implementation of ISO27001.

What is ISO27001?

ISO27001 is a holistic information security framework that organisations can deploy to help them thoroughly to protect their data, and the data of their clients and employees.

The framework is concerned with almost any type of threat to data, including ransomware and other digital attacks, but also - for example - destruction by an employee error or office fire.

It is 'holistic' because although it covers what you might expect (such as firewalls, anti-virus, and secure encryption), it also deals with a range of other aspects of information security, including physical security and mitigation of risks around negligent or disgruntled employees.

**Anti-virus and other technical security measures make up what is known as 'cybersecurity', and cybersecurity is a sub-set of information security.*

What are the benefits - why do people do it?

Implementation of ISO27001 substantially increases the level of information security in an organisation. This is obviously a good thing in itself, but the certification is also useful as evidence to potential customers and investors that your business will look after their sensitive data. Indeed, some companies will only do business with or invest in organisations that are certified to ISO27001 or similar.

ISO27001 may also be a constructive influence outside the realm of security in the growth of smaller companies - a kind of management consultancy tool. For example, it can provide guidance regarding development of the HR function, relationships with suppliers and third parties, and so on.

What kind of companies tend to be interested in ISO27001?

Companies that…
>> store, manage or process high value data (health, legal, financial, intellectual property)
>> are in sensitive industries (banking, media, energy, telecoms etc.)
>> have high-profile online platforms with many users spending money there (gambling, gaming, crypto)
>> are suppliers of services to organisations in one of the above sectors or which are government or regional/local authority entities (e.g., councils)
>> are involved in software development

* Also: Other certifications such as SOC2 and GLI-33, and selection and deployment of software solutions.

robin.long@kiowa.tech

What does implementation entail?

The cost and length of time that it takes to implement ISO27001 and subsequently achieve certification depend on a number of variables. These include the size of the organisation, the type of business that it's in and the time and commitment that are available.

In order to calculate an accurate estimate of pricing and project duration, it's necessary to do a risk assessment and gap analysis of the organisation's existing information assets, roles and responsibilities and relevant documentation, processes and technical measures that it has in place.

What does Kiowa do?

Kiowa undertakes the following required steps of implementation:

* Assessment of the current information security status of the company, and gap analysis against ISO27001; estimate of project duration, price and required client engagement

* Risk assessment and preparation of the Information Asset Inventory and Statement of Applicability

* Assistance with implementation of requirements and applicable controls, and advice regarding potential solutions including software solutions

* Preparation of documentation

Note that there is a substantial volume of documentation that is required for the standard, including but not limited to: Information Security Policy; a number of sub-policies including Access Control, Cryptography, Change Management, Business Continuity/Disaster Recovery; modifications to Contract of Employment, Employee Handbook and NDA template.

* Internal audit prior to certification

* Interaction with certification auditor for certification audit

Other ISO27001 services

If you don't currently have the time or inclination to do the full ISO27001 implementation and certification, Kiowa can help you to develop one or more specific areas of your information security posture. These might be, for example, HR security, secure development or building an asset inventory. For many organisations, step-by-step is the most appropriate way to work towards full certification.

robin.long@kiowa.tech