

# ISO 27001

## Effective information security management

**Effective information security management ensures that the confidentiality, integrity and availability of information held throughout your organisation is preserved.**

ISO 27001 is the information security standard that is now the benchmark for global best practice. This two-part standard refers to both electronic and paper-based information, and covers a wide range of security considerations including personnel, the physical environment, business continuity planning and systems access, development and maintenance.

Implementing a recognised information security management standard, such as ISO 27001, provides you with a framework to manage the security of your information and minimise both internal and external threats, benchmarking your organisation's security standards against best practice.

It provides existing and potential customers and regulators with the assurance that your information and systems are secure, demonstrating credibility and trust and illustrating a commitment to ensuring continuous high levels of information security. It can also significantly reduce the risk and severity of security incidents.

The effective management of information in a secure manner is fundamental to any organisation and ISO 27001 (BS7799) provides an excellent framework to achieve this.

**Through our detailed approach we work with organisations to:**

- Identify the key threats they face;
- Advise on the appropriate level of security required and how to manage their risks;
- Assist in the implementation of those measures needed to protect its business.



### Case study

This construction company serves the international markets for rail, road, utility systems, buildings and complex structures. It provides engineering, construction and service skills to customers for whom infrastructure quality and reliability are critical.

#### Challenge

IT systems and applications are critical to the successful running of the organisation's pensions department, with particular mission critical dependence on the HR and financial systems.

As the information stored on these applications is often confidential and sensitive in nature, the department wanted to ensure the proper governance of this area of business and formalise the processes by which it currently handles and retains this data.

As well as developing and implementing appropriate policies, it also wanted to achieve certification to ISO 27001 (the international standard for information security) at the same time.

A spokesperson for the organisation commented: "Compliance to this standard sends a strong message to our staff and customers that we are serious about our information assurance and it will ultimately ensure that confidential and sensitive information is kept secure."

#### Solution

Having worked with IT consultancy NCC Group on various projects in the past, as well as in an ongoing strategic IT support capacity, the organisation chose to remain with the trusted IT advisor moving forward for the ISO 27001 project.

The NCC Group team worked with the organisation to gain an understanding of its current position and the scope of the project in hand. Following a complete review of the existing information security policies in place, the NCC Group team was able to identify which areas needed to be addressed in order to achieve ISO 27001 compliance.

The team then performed a gap analysis, supplemented by recommendations for how the changes should be made and implemented an action plan and prioritised route map for achieving these objectives.

#### Results

As a result, the company achieved ISO 27001 certification within a year and has compliant policies in place for the ongoing management and security of its information.

The spokesperson commented: "We've always had a great relationship with NCC Group and knew with the team's advice we would be able to efficiently and effectively secure our critical information assets, and reach our objective of becoming ISO 27001 compliant. We now have peace of mind that our key information assets are appropriately and effectively protected."