

Why is a certified ISMS important?

A company's assets include sensitive and highly classified data. A company's assets translate into strength, power, competitive edge and profitability. *“Good corporate governance demands that business leaders have a duty to consumers, shareholders, employees and society as a whole to make effective information security and safety a high priority. Put simply, companies who build trust will win, those that do not will lose.”* ~ Dame Pauline Neville-Jones – Info Breeches Survey ~

The ISMS ensures that assets and the infrastructures around the data are adequately protected against threats. It ensures a system of implementing, operating and monitoring security that covers policy, procedures, processes and reviews.

Establishing an ISMS is a strategic business decision that can reap benefits and profits for the company. The impact of an incident can be devastating.

Most organizations find that following implementation; they have a full understanding where the information is within their business, how it flows through the organization, and what the response plan will be moving forward. This allows them to take ownership and control of the processes and procedures and health of the infrastructure.

Key drivers in the industry for implementation

- Concerns about the security of Internet accessibility
- Information breaches, are reported on a daily basis in the news about many businesses
- Site hacking
- Supply Chain pressure
- Industry competition - certification can be used as marketing tool, providing product or service differentiation
- Insurance premium reductions
- Information terrorism
- **Due Diligence and Litigation Readiness**

Advantages of an ISMS

Organization	Commitment: certification serves as a guarantee of the effectiveness of the effort put into rendering the organization secure at all levels, and demonstrates the due diligence of its administrators.
Legal	Compliance: certification demonstrates to competent authorities that the organization observes all applicable laws and regulations. In this matter, the standard complements other existing standards and legislation (for example HIPAA, the Privacy Act of 1974, the Computer Security Act of 1987, the National Infrastructure Act of 1996, the Gramm-Leach-Bliley Act of 1999, and the Government Information Security Reform Act of 2001) and SARBANES-OXLEY
Operating level	Risk management: leads to a better knowledge of information systems, their weaknesses and how to protect them. Equally, it ensures a more dependable availability of both hardware and data.
Commercial	Credibility and confidence: partners, shareholders and customers are reassured when they see the importance afforded by the organization to protecting information. Certification can help set a company apart from its competitors and in the marketplace. Already, contracts are starting to require ISO 27001 certification.
Finance	Reduced costs related to security breaches, and possible reduction in insurance premiums and possible shield from legal action.
Employee Engineering	Improves employee awareness of security issues and their responsibilities within the organization. Assigns accountability and ownership.