What is an information security management System (ISMS)?

1 A centrally managed framework for keeping information safe.

2 Protects the confidentiality, availability and integrity of information.

3 Consists of a set of policies, procedures, technical and physical controls.

4 Can either be applied to the entire organisation or only a specific area or department (the scope).

5 Based on an organisation-wide risk assessment that considers internal and external risks.

6 All risks are assessed, analysed and evaluated against a set of predetermined criteria.

7 Controls are applied to treat risks based on the likelihood and impact of the risks.

8 Controls can include technology as well as controls to manage people, resources, assets and processes.

9 Helps you control risks that are specific to your own business environment.

10 Requires support and involvement from the entire business from the cleaner right up to the CEO.

11 Managing an ISMS is not an IT function but a business management process.

12 Requires constant review, monitoring, audits and continual improvement to be effective.

13 The international information security standard, ISO 27001, offers best-practice guidance for implementing an ISMS.

Achieving accredited certification to ISO 27001 demonstrates to your clients, customers, regulators and stakeholders that your organisation is following information security best practice and your data is sufficiently protected.

Find out about the benefits of implementing an ISO 27001-compliant ISMS.

Find out how to get started with implementing an ISMS today