Article

Oct 2022

ISO27001 – worth it, or a pain in the annex?

Information security, cyber security and privacy protection remain high on the strategic agenda for most companies. ISO 27001 is changing. We find out how the new standard can help protect your business.

Simon Evans
Principal Security Consultant

Email simon.evans@waterstons.com

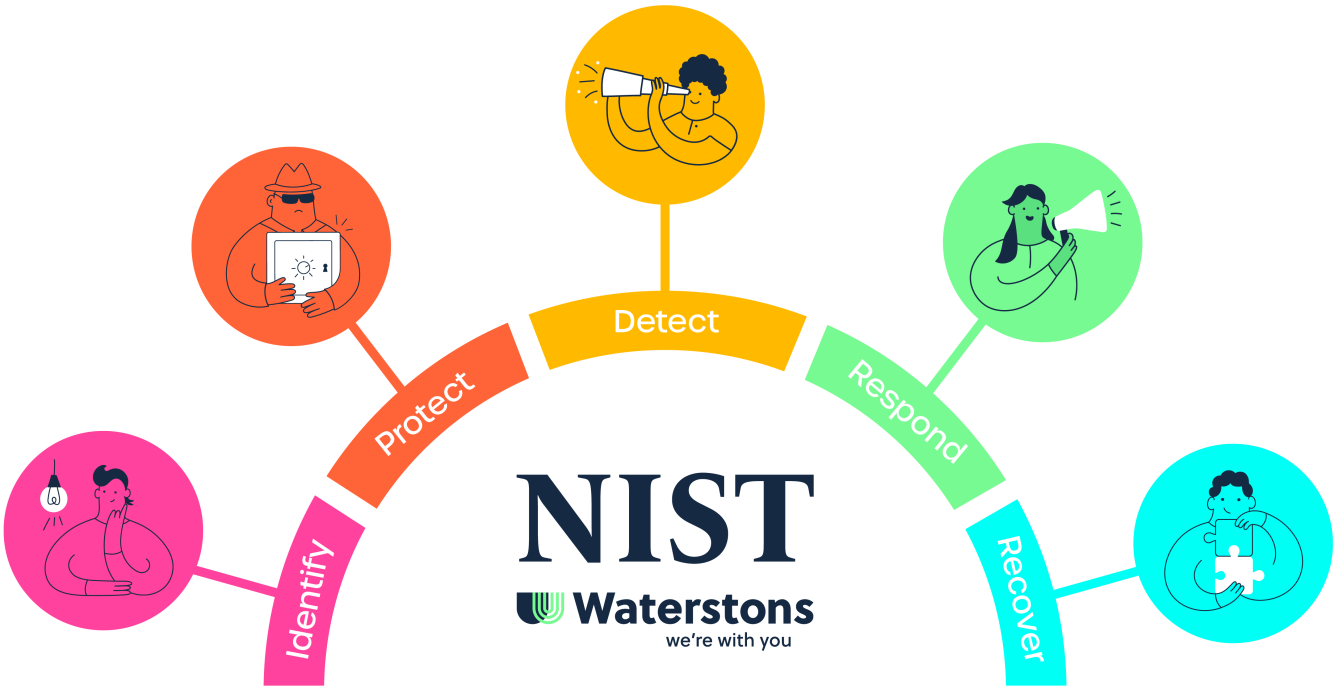
What is ISO27001 and why has it changed?

This international standard specifies the requirements for establishing, implementing, maintaining and continually improving an effective information security management system (ISMS). It assists organisations in protecting the confidentiality, integrity and availability of their information assets. Every ISO Standard undergoes periodic reviews to ensure they are fully up to date with the way we live and work. The cyber security industry is continually evolving and as such ISO 27001 has been updated to reflect a harmonized approach with other Management System Standards and other cyber security framework concepts.

ISO 27001

ISO high level management structure

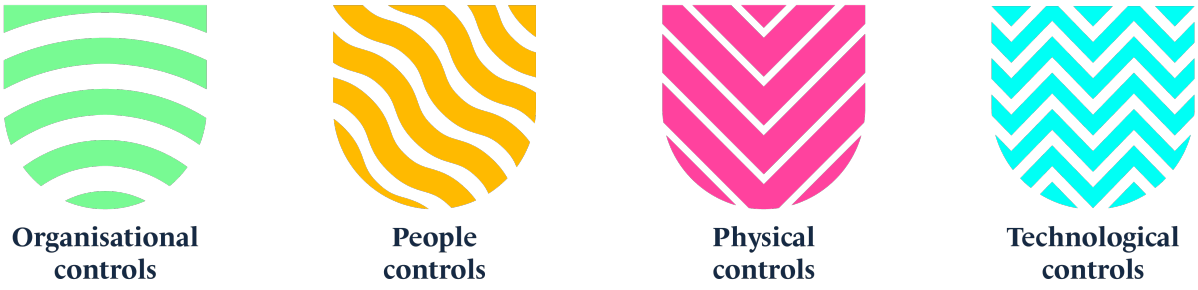
Cyber security concepts



The high-level structure of ISO27001 continues to be similar to that of other ISO standards, such as ISO9001 for quality management, and follows the plan/do/check/act cycle for continual improvement. There have been minor changes to this high-level structure for the 2022 update of ISO 27001.

Significant changes have been to the Annex A control set to allow a different way of viewing the controls. This control set has been reduced from 114 to 93 controls over four domains.

New ISO 27001 control domains



ISO27001 continues to require an organisation to:

- Systematically examine their information security risks
- Implement effective information security controls to address risks
- Monitor ISMS performance to ensure it continues to meet information security needs
- Apply continual improvement activity to the ISMS
- Consider of the application of a series of Information, Cyber and Privacy controls

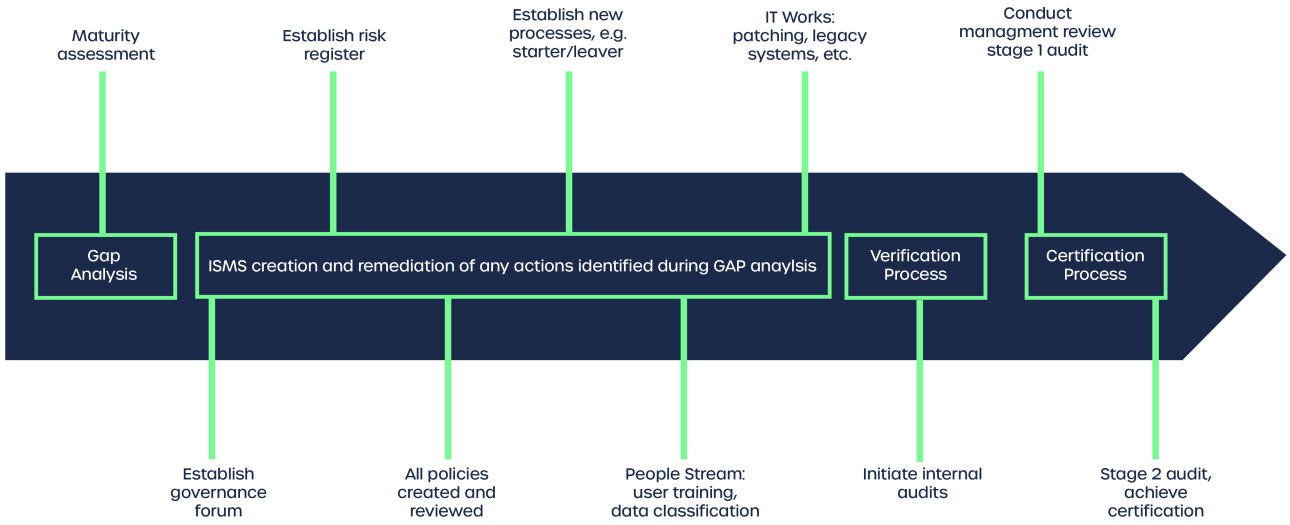
What are the benefits of ISO27001?

It shows your organisation:

- Is committed to improving information security for clients, suppliers and employees
- Has enhanced its risk management and is able to identify threats
- Is prepared to defend itself - and its reputation - during and after an information security incident
- Has built a robust security culture
- Has international recognition, putting it in a potentially stronger position when it comes to tender opportunities.

How long will it take to get certified?

There is no set timescale to achieve formal certification as it is dependent on the size and complexity of the information security management system, current levels of maturity, and availability of monitoring and measurement results to demonstrate compliance. Below is an example of the typical timeline for certification.



Certification timeline

We have a team highly experienced professionals to help you start, strengthen or continue your information security management system journey.

Whether it's an assessment of your current security posture, staff awareness training, assistance with an ISO27001 compliant policy document set, development of risk management processes, or a side-by-side partnership leading you through to formal ISO27001certification and beyond, we're with you.

For more information on who we are and what we can offer, click here.