

# ISO 27001 certification

A number of certification bodies are accredited by national standards bodies (such as the British Standards Institution and the National Institute of Science and Technology) to review compliance with ISO 27001 and issue certificates. [Around 1,800 organizations worldwide](#) have already been certified against BS 7799 part 2 (or their national equivalents) and the pace of adoption is increasing.

Organizations can specify the scope of their ISO 27001 certification as broadly or as narrowly as they wish. Understanding the scoping documents (known as “Statements of Applicability”) is therefore crucial if one intends to attach any meaning to the certificates. If an organization’s ISO 27001 SOA only notes “Acme Ltd. Department X”, for example, the associated certificate formally says nothing about information security in “Acme Ltd. Department Y”.

Certification is entirely optional but is increasingly being demanded from suppliers and business partners by organizations that are concerned about information security. Certification against ISO 27001 brings a number of benefits above and beyond simple compliance, in much the same way that an ISO 9000-series certificate says more than “We are a quality organization”. Independent assessment necessarily brings some rigor and formality to the implementation process (implying improvements to information security and all the benefits that brings through risk reduction), and invariably requires management approval (which is an advantage in security awareness terms, at least!). The certificate has marketing potential and should help assure most business partners of the organization’s status with respect to information security without the necessity of conducting their own security reviews.