ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEMS
AUDIT, CERTIFICATION & TRAINING SERVICES

SGS

HOW CAN YOU KEEP YOUR INFORMATION SAFE OVER THE LONG-TERM?

ISO 27001 AUDIT, CERTIFICATION & TRAINING SERVICES FROM SGS

Most, if not all, organisations today could not function without modern and secure information and technology systems. Any disruption in the quality, quantity, distribution or relevance of your information and data can put your business at risk. The security of information systems and business-critical information must be actively and constantly managed in order to ensure the continuity of your operations and the safety of your data and systems. That is a challenge, but it is also a chance for you to stand out from the competition and demonstrate a strong culture of information security management.

ABOUT ISO 27001:2005

The ISO 27001:2005 Information Security Management Systems (ISMS) standard considers everything about risk. There are three core principles involved: confidentiality, integrity and availability, which cover eleven areas:

- Security policy;
- Organisation of information security;
- Asset management;
- Human resources security;
- Physical and environmental security;
- Communications and operations management;
- Access control;
- Information systems acquisition, development and maintenance;
- Information security incident management;

- Business continuity management; and
- Compliance.

The first step in achieving ISO 27001:2005 certification is to define the scope of your ISMS policy. This is critical to identifying the dangers you face and for deciding upon a systematic approach as to how to assess these risks. A successful ISMS includes standard steps for implementation, operation, review, maintenance and system improvement.

THE BENEFITS

Certification against ISO 27001:2005 enhances the credibility of your organisation and demonstrates the integrity of your data and systems and your commitment to information security.

It can also transform your organisation's culture both internally and externally, opening up new business opportunities with security conscious customers, improving employee ethics and strengthening the notion of confidentiality throughout the workplace. Furthermore, it allows you to enforce information security and reduce the possible risk of fraud, information loss and disclosure.

HOW DOES THE CERTIFICATION PROCESS WORK?

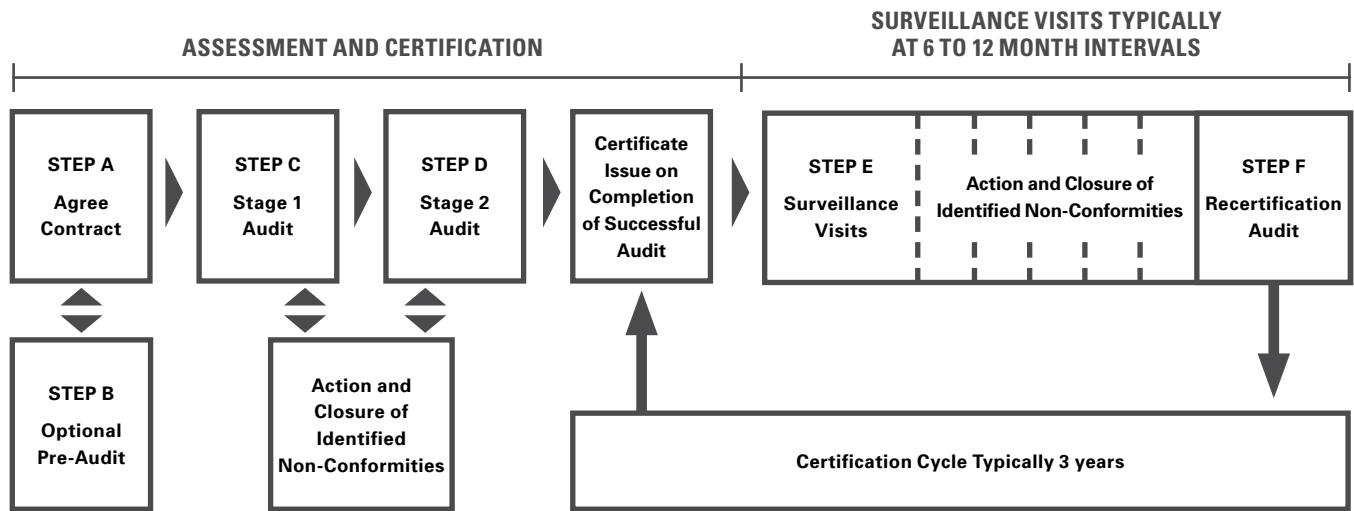The ISO 27001:2005 certification process consists of six steps:

- Step A – SGS provides you with a proposal based on the size and nature of your organisation. You can then proceed with the audit by accepting the proposal.
- Step B – You may ask SGS to perform a 'pre-audit' to give an indication of the readiness of your organisation for the audit. This stage is optional, yet it is often found useful in identifying any weaknesses in your systems and in building confidence before the formal audit.

- Step C – The first part of the formal audit is the 'Stage 1 – Readiness Review'. This lets us evaluate the compliance of your documented system with the requirements of the standard to better understand the nature of your organisation, to plan the rest of the audit as effectively as possible and to initially examine key elements of the system. You will receive a report after this stage identifying any concerns or observed non-compliances so that you can take immediate action if required.
- Step D – This is 'Stage 2' of the initial audit process. The audit includes interviews with you and your colleagues and examination of records. Observation of your working practices determines how compliant your actual processes are with the standard and with your own documentation system. At the end of this stage, we will present the findings of the audit classified as either major or minor non-conformances along with other observations and opportunities for improvement. Once you have addressed the non-conformities, a technical review of the audit will then be conducted by an authorised SGS Certification Manager to confirm the issuance of a certificate.
- Step E – Our surveillance visits will be scheduled at either six or twelve month intervals depending on the contract. During the visits, we review the implementation of the action plan addressing the past non-conformities and examine certain mandatory and other selected parts of the system in line with an audit plan that we provide you before each visit.
- Step F – Shortly before the third anniversary of the initial certification, our routine visit will be extended to enable a re-certification audit. Surveillance visits will then continue, as before, on a 3-year cycle.

ISO 27001:2005 CERTIFICATION PROCESS

ASSESSMENT AND CERTIFICATION

SURVEILLANCE VISITS TYPICALLY AT 6 TO 12 MONTH INTERVALS

| STEP A Agree Contract | STEP C Stage 1 Audit | STEP D Stage 2 Audit | Certificate Issue on Completion of Successful Audit | STEP E Surveillance Visits | Action and Closure of Identified Non-Conformities | STEP F Recertification Audit |

| STEP B Optional Pre-Audit | | Action and Closure of Identified Non-Conformities |

Certification Cycle Typically 3 years

ISO 27001:2005 RELATED TRAINING

We offer a wide variety of training courses for all levels of ability and awareness. Our ISO 27001:2005 training course portfolio is designed to meet the requirements of any organisation using ISO 27001:2005, and includes:

- ISMS Introduction & Awareness (IRCA accredited);
- Internal ISMS Auditor (IRCA accredited);
- ISMS Auditor Conversion (IRCA accredited);
- ISMS Lead Auditor (IRCA accredited); and
- ISMS architecture and project management.

Please visit www.uk.sgs.com/training to view the ISO 27001:2005 course schedules in your region.

OTHER SERVICES RELATED TO INFORMATION SECURITY MANAGEMENT SYSTEMS

SGS is also known for its solutions against other needs related to management systems like quality, the environment, IT service and business continuity:

- Maturity level: SGS can help you to identify and determine the maturity level of your current ISMS in order to ensure continual improvement or to initiate a project. An assessment report will be provided with a radar chart, objective findings and constructive conclusions. It would be advised to take a full scan either prior to the ISMS project or annually to identify progress and achievement;
- Business Continuity Management (BS 25999) standard audit, certification and training services;
- Integrated Management Systems: ISO 27001:2005 can be adopted in all types and sizes of organisations. Your ISMS can be audited and certified simultaneously with other management systems which you have implemented; and
- Audit solutions against additional, bespoke information security controls: SGS can help develop the performance criteria and the checklist or simply check performance against existing measures.

WHY SGS?

SGS is the world's leading inspection, verification, testing and certification company. Recognised as the global benchmark for quality and integrity, we employ over 67 000 people and operate a network of more than 1 250 offices and laboratories around the world. We are constantly looking beyond customers' and society's expectations in order to deliver market leading services wherever they are needed.

Partnering with SGS opens the door to better performing processes, increasingly skilful talent, consistent and compliant supply chains and more sustainable customer relationships delivering profitable competitive advantage. Work with the global leader and take your commitment to the next level.

We have a history of undertaking and successfully executing large-scale, complex international projects. With a presence in every single region around the globe, our people speak the language and understand the culture of the local market and operate globally in a consistent, reliable and effective manner.

TO LEARN HOW SGS CAN HELP YOU EXCEED CUSTOMER EXPECTATIONS, VISIT WWW.UK.SGS. COM/INFORMATION-SECURITY-MANAGEMENT OR CONTACT UK.NOWISTHETIME@SGS.COM FOR MORE INFORMATION.

WWW.SGS.COM

WHEN YOU NEED TO BE SURE

SGS