

## Information security management system certification: the industrial sectors concerned and areas of focus

The correct management of security is now a critical element for all companies that look on their information and company assets as resources to be protected. Therefore, companies must identify specific critical elements according to the goods sector they operate in.

### Financial sector

The world of financial services incorporates different sectors, from banks to insurance companies, which all share the need to use network systems to carry out monetary transactions and to exchange information. Distinguishing elements are:

- Transaction protection.
- Data protection.
- Electronic payments.

Financial companies that are not able to provide adequate levels of security risk various types of deception and exposing their customers to the dangers of IT fraud.

### Industrial sector

As a result of the rapid spread of IT in the manufacturing sector, IT system security is emerging as one of the priorities for companies operating in the more traditional industrial sectors.

In the manufacturing world, the following distinguishing features can be identified:

- B2B Marketplace
- Remote access for workers
- Legislative constraints in particular sectors (chemical, armaments, agro-industry)
- Industrial espionage

Protection of industrial secrets is therefore one of the main critical areas for the manufacturing industry, which means there is an obvious need to protect intellectual property.

### Public sector

The public sector groups together many different areas, for which the issue of IT system security is of fundamental importance; in particular, these concern public administration (PA), strictly speaking, defence and health.

For PA, the areas of interest concern e-government projects and relations with the public, with companies and between internal departments. All initiatives are highly Internet-based with elevated risks of service interruption. So, in terms of security, transaction management and the security of Internet and public intranet access



are reiterated among the priorities.

For the defence sector, urgent problems linked to security regard the reliability of maximum security systems and protection against attacks, both virtual attacks on networks and physical ones on infrastructures.

The integrity of information is also a critical issue for the health sector, which must implement efficient access control systems, at the same time ensuring the availability - to industry professionals - of sensitive patient information. This involves the need to focus on both organisational and IT security (access control, communications, computer protection) solutions.

### IMQ profile

The IMQ Group is Italy's leading organisation in conformity assessments (certification, tests, verification and inspections).

With a strong synergy among group companies, expertise gained in more than 50 years of experience, and a complete range of services on offer the IMQ Group is the partner of choice for companies whose goal is safety and quality.

The IMQ Group operates in numerous sectors, from the electro-technical and electronics industries to telecommunications, the automotive sector, the gas appliance, plant engineering, construction products and agricultural and food industries. The Group provides wide-ranging and specific, targeted services, including product certification, conformity assessment to EC directives, company management system certifications, inspections of



systems and buildings, laboratory tests and tests to obtain international approvals, assistance with exports, surveillance of manufacturing abroad, assistance with technical formalities and standards, as well as training.

The comprehensive range of services is delivered through IMQ Group companies located throughout Italy and abroad operating for different product categories, comprising: IMQ S.p.A. (Milan - Italy), CSI S.p.A. (Bollate - Italy), IMQ Primacontrol S.r.l. (San Vendemiano - Italy), IMQ Klima S.p.A. (Amaro - Italy), ICILA S.r.l. (Lissone - Italy), IMQ Iberica (Barcelona - Spain), IMQ Krakow R.O. (representative office based in Poland), IMQ Shanghai R.O. (representative office based in Shanghai - China). The IMQ Group also has holdings in Istituto Giordano S.p.A. (Bellaria - Italy), in CISQ-CERT S.p.A. (Milan - Italy) and Icube S.A. (Buenos Aires - Argentina).



Via Quintiliano, 43 - 20138 MILANO - Italy - Tel. + 39 02 5073222- Fax +39 02 50991544  
commerciale.csq@imq.it - www.imq.it

Mod. 576/E/0 - 2009/05



Information Security Management System Certification  
ISO 27001 standard

# Information Security Management System Certification - ISO 27001 standard

“ Thanks to vast experience gained in the wider production environments, CSQ is able to provide companies with dedicated services that are sensitive to the issue of security which compare their solutions against ISO 27001, the reference standard for information security. ”



Information system security is today one of the priorities for many companies who operate in national and international economic environments. Not all companies, however, are aware of the range of benefits that a security system can bring, not just to the company's IT infrastructure, but to intellectual property assets.

An assessment of security needs is the ideal starting point for drawing up the most suitable solutions to meet the needs of every company. In fact, if the new economy has led to a considerable speeding up of interactions in electronic format (typical examples are those of the banking, insurance and tourism sectors) and therefore to a need for transaction security, the protection of privacy has also meant that hard-copy archives must be subject to the minimum security requirements (as extensively confirmed by Law 675/96, Presidential Decree 318/99 and by the new Personal data protection code 196/03).

By now, it is well known that security cannot be achieved and guaranteed solely through technical means (firewall, antivirus, encryption and digital signatures); and so it becomes critical to implement an Information Security Management System (ISMS) based on a set of controls derived from company policies and to be applied to all business and support processes.

## Regulatory and legislative overview for information security

Italian legislation, which governs the processing of personal data, the identification of minimum security measures, copyright, legal protection of computer programs, digital signatures and the use of certified e-mail, is summarised in the following main acts.

### Directive compliance

- Legislative Decree no. 518 of 29/12/1992 which modifies Royal Decree no. 633 of 1941, relating to copyright, integrating it with regulations on the legal protection of computer programs.
- Law no. 547 of 23/12/1993 which modifies the Italian Penal Code introducing the theme of computer crimes.
- Law no. 675 of 31/12/1996 which governs the processing of Personal Data (Privacy Law).
- Presidential Decree no. 513 of 10/11/1997 regarding regulations on electronic documents and digital signatures.
- Presidential Decree no. 318 of 28/07/1999 Regulation introducing rules for the identification of minimum security measures for the processing of Personal Data, pursuant to article 15, paragraph 2, of Law no. 675 of 31/12/1996.
- AlPA (Authority for IT in Public Administrations) Resolution 42/2001, 13 December 2001 and Explanatory Notes (Official journal no. 296 dated 21-12-01) Object: Technical specifications for the reproduction and storage of documents using optical media suitable for guaranteeing conformance of the documents with the originals - article 6, paragraphs 1 and 2, of the Consolidated act of legislative and regulatory provisions on administrative documentation, pursuant to Presidential Decree no. 445 of 28 December 2000.
- Legislative Decree no. 10 (Official journal no. 39 of 15 February 2002) Implementation of directive 1999/93/EC relative to a community framework for electronic signatures.
- Presidential Decree no. 137 of 7 April 2003 (Official journal no. 138 of 17 June 2003) Regulation introducing coordination provisions on electronic signatures pursuant to article 13 of legislative decree no. 10 of 23 January 2002.
- Legislative Decree no. 196 of 30 June 2003 (Personal data protection code).
- Decree of the President of the Council of Ministers of 13 January 2004 (Official journal no. 98 of 27 April 2004) Technical specifications for the creation, transfer, storage, duplication, reproduction, and validation, including by time-stamp, of electronic documents.
- Presidential Decree no. 68 of 11 February 2005 (Official journal no. 97 of 28 April 2005)

Furthermore, we should point out the EEC normatives on security

- Regulation introducing provisions on the use of certified e-mail, pursuant to article 27 of law no. 3 of 16 January 2003.
- Directive 97/66/EC of 15/12/1997 on the processing of Personal Data and protection of privacy in the Telecommunications sector.
- Directive 96/9/EC of 11/03/1996 relative to the "Legal protection of databases".
- Directive 95/46/EC of 24/10/1995 relative to the "Protection of individuals with regard to the processing of Personal Data, and on the free movement of such Data".

Voluntary regulations:

- ISO 27001 (ex BS7799 - part 2) Information Technology Security Techniques
- ISO 27002 (ex BS7799 - part 1) Information Technology Code of practice for Information Security Management.



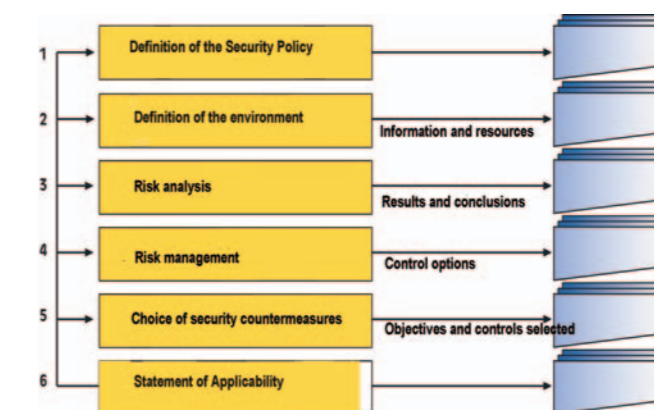
## CSQ-DATA certification scheme

For the purpose of issue of the ISO 27001 certification, CSQ has developed an appropriate scheme called CSQDATA.

CSQ-DATA is a scheme that allows Organisations to certify their own Information Security Management System (ISMS), evaluating the following aspects in particular:

- Security Policy
- Vulnerability analysis and risk management
- Existence of an organisation dedicated to security
- Definition of useful controls in implementing security
- Security management procedures
- Evaluation and periodic review of the ISMS adopted.

### STEPS IN IMPLEMENTING AN INFORMATION SECURITY MANAGEMENT SYSTEM



### The certification process

This generally happens in at least two stages, both to determine compliance with ISO 27001.

#### Stage 1: Document review

Evaluation of the documentation to support the ISMS, from the security management manual to the risk analysis document. This can be carried out at the organisation's offices and pertains to all the main documentation of the Information Security Management System (ISMS).

#### Stage 2: Audit of the organisation

Company visit based on interviews, review of documents, comparisons between formalised procedures and operating practices. The goal is to verify that the organisation adheres to its own policies, objectives, procedures and that the ISMS is effective.

## Objectives

To protect Data and Information from a wide variety of threats (unauthorised access, destruction and theft of data, service interruption, computer viruses) in order to ensure continuity of company activities. Possessing an accurate information security management system means being equipped with all the security measures, ensuring data in terms of confidentiality, integrity and availability.

- Confidentiality: so that all information is only accessible by authorised individuals
- Integrity: to prevent undue, accidental or fraudulent changes to information
- Availability: to ensure that users can access databases on the basis of the specific profiles enabled in times in line with their operating needs.

## The benefits of the CSQ-DATA certification

The information security management system certification makes it possible to:

- facilitate compliance with contractual and legislative requirements
- reinforce the company's credibility and visibility by protecting its image and assets and facilitating the retrieval of information
- manage the costs of security incidents
- effectively finalise investments used to implement security controls
- ensure and provide proof to stakeholders that all the tools and technical and organisational measures necessary to guarantee Information Security have been implemented.

## IMQ accreditations

The main goals achieved by IMQ in the field of IT security accreditations are:

- IMQ is the certification body accredited by SINCERT (National System for the Accreditation of Certification Bodies) to issue certificates in compliance with the ISO 27001 standard in all sectors that meet the EA (European Cooperation for Accreditation) international classification.
- IMQ's Security Testing Laboratory is able to perform assessments of IT security in line to Common Criteria (ISO/IEC 15408) and ITSEC standards. It is accredited in the National Scheme for the Evaluation and Certification of the Security of ICT systems and products.