alliuris

ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS

# IT Security according to ISO-27001

*Ulrich Herfurth, Lawyer in Hanover, and Brussels*
*Eduardo Isaac Soto Barrera, Lawyer (Mexico) Mag. iur. (Mx), Mag. iur. (D), Hanover*

*July 2021*

To be competitive in the market, it is evident that it is essential to offer advantages that set a company aside from the rest. In the area of IT security, for many providers, partners, and customers, even trust is not sufficient, but rather a certification is. This implies that the company publicly commits to high standards in data and information security.

The benefits of certification are obvious: increased competitiveness on a national and international level and the minimisation of risks for security threats, which represent an investment in the medium and long term.

However, companies should not be in a rush to just obtain a certification. The implementation of such systems must be regular and gradual in each department or in management in general.

## The ISO 27001 standard on IT security

This standard is still the default choice for small and medium-sized enterprises when implementing an ISMS (Information Security Management System), compared to certification by means of the BSI Compendium. Companies can set up their system according to the ISO 27001 standard - and have it certified.

This standard comprises 11 chapters and an Annex A. In total, it contains 32 mandatory sheets, 250 option sheets and 114 controls that have international recognition. Certificates are valid for up to three years, after which they can be renewed. It could be extended for only one or two years, provided that annual audits are conducted in certain cases. This type of accreditation has specific features that the company must take into account beforehand: it can be addressed to the company as a whole or to specific departments, it is not dependent on another certification such as ISO 9001, and its implementation requires a high level of commitment to policy development within the company. Its focus is on the following measures: Context of the organisation, Implementation, Planning, Support, Operation, Evaluation of performance and Improvement, which can be used as guidelines in this category. For practical reasons, we will mention only some of these aspects.

### *Context of the organisation*

It must consider the purpose and activity of the organisation, including its consequences. It considers possible influencing external and internal activities, especially financial aspects, technological dependencies, supply chains or even contractual relationships.

This flexibility is one of the advantages compared to the BSI guidelines. ISO 27001 adapts to the characteristics of the company, which experts believe is common in the technology industry and start-ups in general.

*Guidance*

The activities and obligations must be described in detail starting from the management itself. The aim: to circumscribe the level of responsibility for information security.

The creation of policies contains the activities, responsibilities, and authorities, including the delegation of activities that are controlled by internal company protocols and communication.

Some appoint a compliance manager who monitors the processes of the IT system and IT operations in terms of the conception and organisation of requirements management, others appoint an IT security officer who is responsible for this monitoring from a different and in some respects even broader perspective in terms of IT security.

However, it should not be forgotten that these agents only assist, because the so-called management level is ultimately the one who must provide a clear line in terms of selecting the most qualified employees, so that the responsibilities, once defined, can also be properly addressed, and corrected in due course.

*Support*

Employees must be informed of the correct forms of internal communication and their options for reporting security incidents to the competent authorities.

In addition, there must be the opportunity to access the necessary documentation in which the risk protocols are classified and in which the weak points, the possibilities for action by the employees and the scope of the measures are listed.

It is also important to note that the measures to be taken must also be assumed by the contractors. They have obligations and responsibilities in the area of information security that may extend beyond the duration of the contractual relationship. To this end, the 'Code of Conduct' also applies to employees and contractors in terms of confidentiality, data protection, necessary use of resources, company business practices, etc. To this end, awareness programmes help to consolidate and revise this knowledge.

In relation to these programmes, there is a mistake companies make of focusing too much on IT and overlooking the human element in their security systems. The most important thing is to protect the information, not the processes. It should not be assumed that the systems are fail-safe and that the staff have necessarily been negligent.

**Features of ISO 27001**

This norm provides flexibility, which translates into a broader scope for the company to design policies and guidelines to protect the information it holds through the 114 controls mentioned above, which can be adapted by users as needed, giving the company greater responsibility.
It also means an increase in competitiveness and efficiency in handling and improving the level of security, as well as minimising the damage that could be caused by physical and computer threats.

Likewise, this certification implies that a comprehensive analysis of the risks and the measures to be taken must be carried out. This analysis includes firstly the identification of the assets (each asset, which was the novelty of the new ISO 27001:2017 to treat information as an asset), including all physical documents, software, hardware, etc., including their acquisition cost, current value, cost in case of loss or theft, etc. Secondly, the vulnerabilities must be disclosed and the financial, legal and other risks that may arise if the assets are compromised must be described in detail.

Furthermore, certification must be realistic in terms of the company's ability to achieve the objectives. Excessive documentation or complexity is counterproductive when applying these guidelines.

**Special features in practice**

In practice, companies must prevent risks. They should generally, but especially in certification processes, avoid having a constant change of personnel. This is seen as a risk not only because in some cases the new staff members do not immediately have the necessary security training (regarding the protection of personal data, the ways to register anomalies in the system or even the lack of knowledge on how to indicate by email that it is confidential information), but also their insufficient understanding of the company culture and how information protection is practiced on a day-to-day basis plays a major role in minimising such risks.

On the other side, if the security risk exists, then the company needs to address the problem in the correct way. The usual approach is to implement an ISMS. The use of so-called "end devices" (computers, tablets, mobile phones and even printers) that are allowed and provided in the workplace present a problem for companies. Some of these devices usually have access to servers and can store confidential information. If they are stolen or lost, this can lead to financial and even legal damages. The company, through an ISMS, should record these events to determine when, where how often, how many of these devices were lost or stolen, and what measures can be implemented to minimise the damage, such as ongoing awareness workshops or limiting the data these devices should contain, using different authentication systems, etc.

Language plays a fundamental role in the way such a standard is interpreted and especially in the time it takes for the ideas of international standards to find their homonyms in other languages. The English term used to be "access", which is imprecise in German. There are three classic definitions of control measures for the same word: "Zutritt, Zugang und Zugriff". Zutritt refers to the physical space where devices such as computers are located, monitored by security camera systems, smart cards to enter facilities, etc. Zugang refers to the systems that are monitored using usernames and passwords, biometrics, etc. Zugriff refers to the extent that users have in the system to access data, IT applications or transactions, regulated by granting administrator rights or the own rules of policies like BYOD (Bring your own device).

Another issue is the criticism of favouring the principle of confidentiality over others. This principle is based on the principle that outsiders should not have access to information that is confidential to the company. However, it is possible for employees, even with the appropriate credentials, to manipulate sensitive company information and data (principle of integrity) intentionally or inadvertently. The principle of "availability" also excludes the prevention of so-called "force majeure", which refers to natural events or phenomena in which devices or data carriers are destroyed, from the scope of this principle. Companies have security concepts where a simple fire can not only cause the destruction of furniture and goods, but also render the information contained in computers and other storage media inaccessible for a variety of reasons, for example: the lack of a backup of information in the cloud. In some cases, the only means of remote access to information by an external company previously contracted by the organisation was a tape drive to which a backup is stored, and which was located in the company's own facilities and cannot be accessed in the event of an earthquake or other disaster. This requires a re-examination of aspects such as a backup.

*Conclusion*

IT security is a specialised field that can be adapted according to the requirements of a company, depending on the industry it belongs to, its internal structure, the type of data it handles, the form of risks, etc. Not to be underestimated are the risks that can arise from the systems and servers, but also from the physical infrastructure itself.

Correct compliance with this standard requires a high level of commitment from management, sufficient resources during the long and arduous journey of certification, and that these guidelines are understood and applied, which is subject to constant review.

Companies need to take advantage of the flexibility of this standard, not only to demonstrate that they have certain technologies or software or knowledge in projects, but also to implement new policies on e-commerce (B2B and B2C) issues, as well as to minimise the damage from cyber-attacks, whether from outside or inside the company.

+++

**ALLIURIS**

The ALLIURIS GROUP consists of 20 law firms and 400 business lawyers within Europe, Asia and America. (www.alliuris.law).

…………………………………………………………………………..

Your contact:
Alisha Daley-Stehr,
Alliuris Communication

info@alliuris.org
Fon 0049-511-307 56-0
Fax 0049-511-307 56-10

…………………………………………………………………………..

IMPRINT

EDITORS

ALLIURIS A.S.B.L.
ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS
BRUSSELS

MANAGEMENT
Luisenstr. 5, D-30159 Hannover
Fon +49-511-307 56-50 505056-20 Fax +49-511-307 56-60

BRUSSELS · PARIS · LONDON · AMSTERDAM · AMERSFOORT . LUXEMBURG · LYON · MADRID · BARCELONA · LISBON · MILAN · COPENHAGEN · HANOVER · ZUG · VIENNA · MOSCOW · MINSK · ATHENS · ISTANBUL · BEIJING · SHANGHAI ·GUANGZHOU NEW DELHI · NEW YORK · MEXICO CITY · SAO PAULO · RIO DE JANEIRO · BRASILIA BUENOS AIRES

EDITORIAL DEPARTMENT
Ulrich Herfurth, Rechtsanwalt

All information is correct to the best of our knowledge; liability is limited to intent or gross negligence. Reproduction, even in excerpts, requires the permission of the editors.