VACO Reference Material

# WHAT IS ISO 27001?

## A SIMPLIFIED GUIDED EXPLANATION ON THE INFORMATION SECURITY MANAGEMENT SYSTEM

Researched and Collated By:
VACO Middle East Est.
Abu Dhabi, United Arab Emirates
info@vaco.ae
+971 56 947 9733
Visit us at www.vaco.ae

Disclaimer: The following pages are extracted from research activity conducted by consultants of VACO Middle East and are reproductions of original work from various industry experts and organizations.

VACO Middle East takes no responsibility with regards to copyright, images, methods, policy and processes, or content as it is reproduced in the best interest of industry benchmarks.

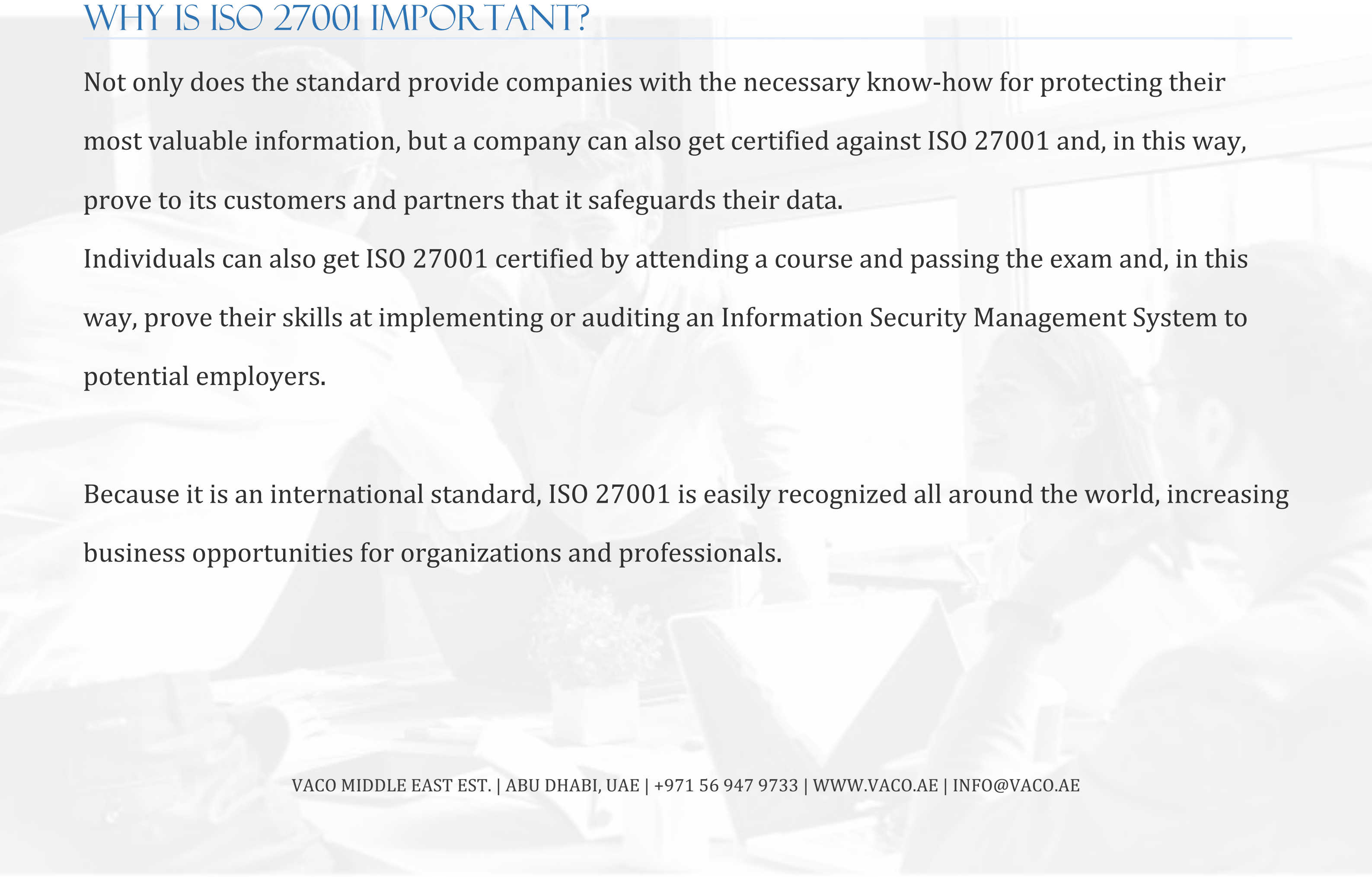
## WHAT DOES ISO 27001 MEAN?

ISO 27001 is the leading international standard focused on information security. It was published by the International Organization for Standardization (ISO), in partnership with the International Electrotechnical Commission (IEC). Both are leading international organizations that develop international standards.

ISO 27001 is part of a set of standards developed to handle information security: the ISO/IEC 27000 series. Its full name is "ISO/IEC 27001 – Information security, cybersecurity and privacy protection — Information security management systems — Requirements."

## ISO FRAMEWORK AND THE PURPOSE OF ISO 27001

The ISO framework is a combination of various standards for organizations to use. ISO 27001 provides a framework to help organizations, of any size or any industry, to protect their information in a systematic and cost-effective way, through the adoption of an Information Security Management System (ISMS).



## WHY IS ISO 27001 IMPORTANT?

Not only does the standard provide companies with the necessary know-how for protecting their most valuable information, but a company can also get certified against ISO 27001 and, in this way, prove to its customers and partners that it safeguards their data.
Individuals can also get ISO 27001 certified by attending a course and passing the exam and, in this way, prove their skills at implementing or auditing an Information Security Management System to potential employers.

Because it is an international standard, ISO 27001 is easily recognized all around the world, increasing business opportunities for organizations and professionals.

## WHAT ARE THE THREE PRINCIPLES OF ISO 27001?

The basic goal of ISO 27001 and an Information Security Management System is to protect three aspects of information:

**Confidentiality:** Only authorized persons have the right to access information.

**Integrity**: Only authorized persons can change the information.

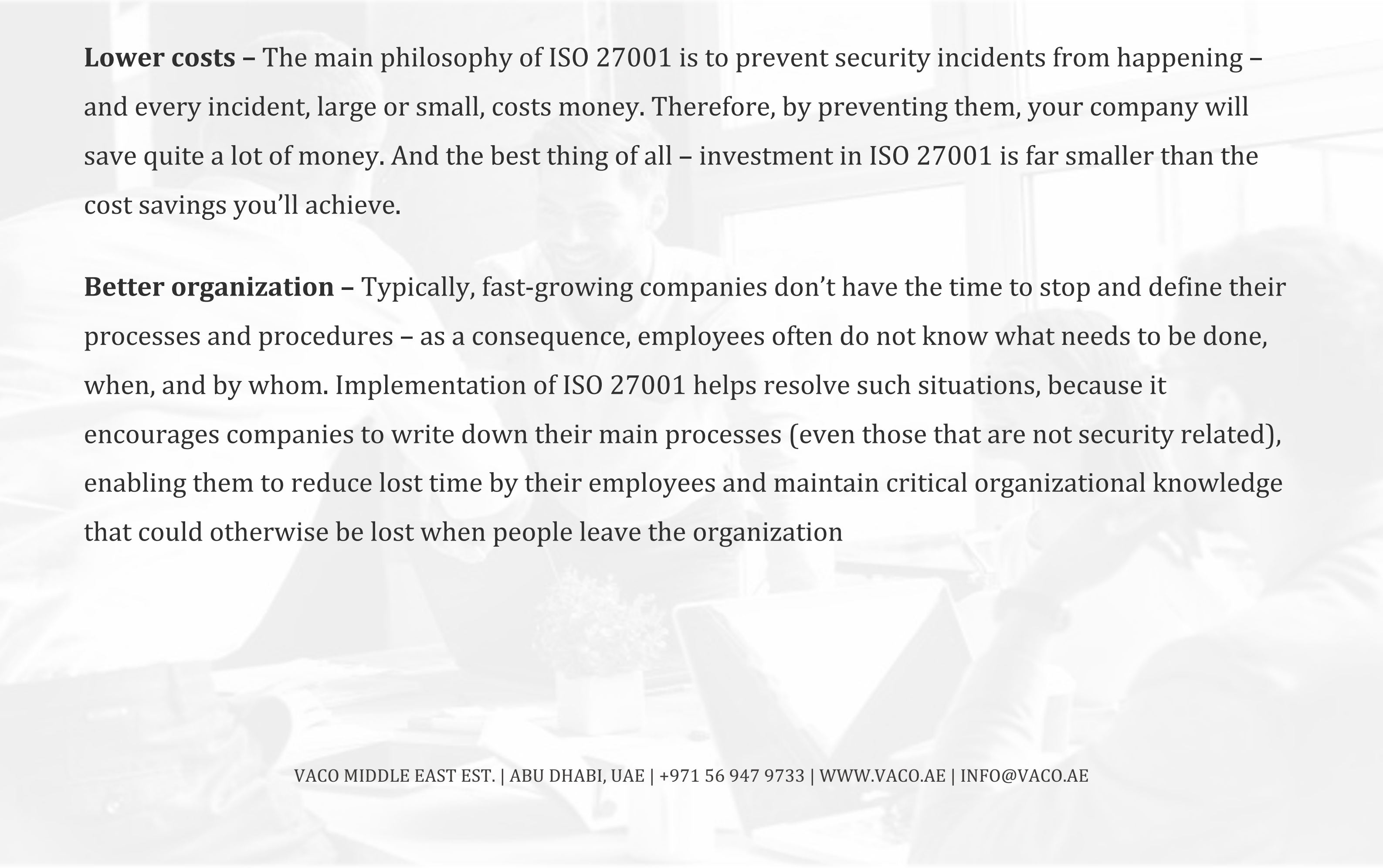
**Availability**: The information must be accessible to authorized persons whenever it is needed.

## WHY DO WE NEED AN ISMS?

There are four essential business benefits that a company can achieve with the implementation of ISO 27001:

**Comply with legal requirements –** There is an ever-increasing number of laws, regulations, and contractual requirements related to information security. The good news is that most of them can be resolved by implementing ISO 27001. This standard gives you the perfect methodology to comply with them all.

**Achieve competitive advantage –** If your company gets certified, and your competitors do not, you may have an advantage over them in the eyes of those customers who are sensitive about keeping their information safe.



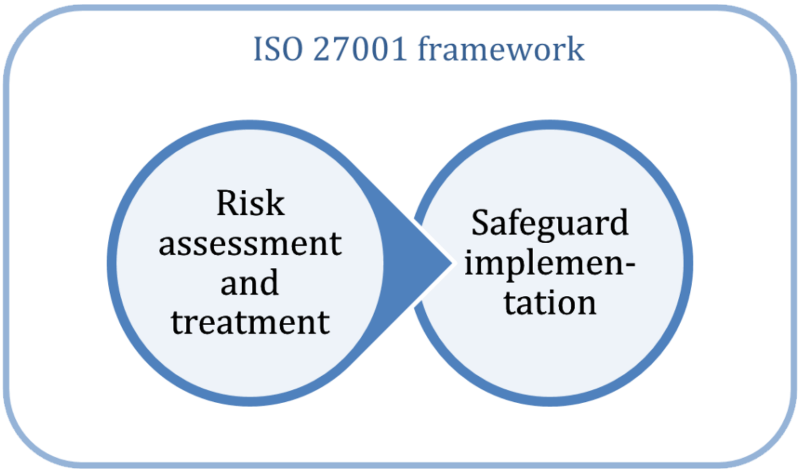
**Lower costs –** The main philosophy of ISO 27001 is to prevent security incidents from happening – and every incident, large or small, costs money. Therefore, by preventing them, your company will save quite a lot of money. And the best thing of all – investment in ISO 27001 is far smaller than the cost savings you'll achieve.

**Better organization –** Typically, fast-growing companies don't have the time to stop and define their processes and procedures – as a consequence, employees often do not know what needs to be done, when, and by whom. Implementation of ISO 27001 helps resolve such situations, because it encourages companies to write down their main processes (even those that are not security related), enabling them to reduce lost time by their employees and maintain critical organizational knowledge that could otherwise be lost when people leave the organization

## HOW DOES ISO 27001 WORK?

The focus of ISO 27001 is to protect the confidentiality, integrity, and availability of the information in a company. This is done by finding out what potential incidents could happen to the information (i.e., risk assessment), and then defining what needs to be done to prevent such incidents from happening (i.e., risk mitigation or risk treatment).

Therefore, the main philosophy of ISO 27001 is based on a process for managing risks: Find out where the risks are, and then systematically treat them, through the implementation of security controls (or safeguards).



ISO 27001 requires a company to list all controls that are to be implemented in a document called the Statement of Applicability.

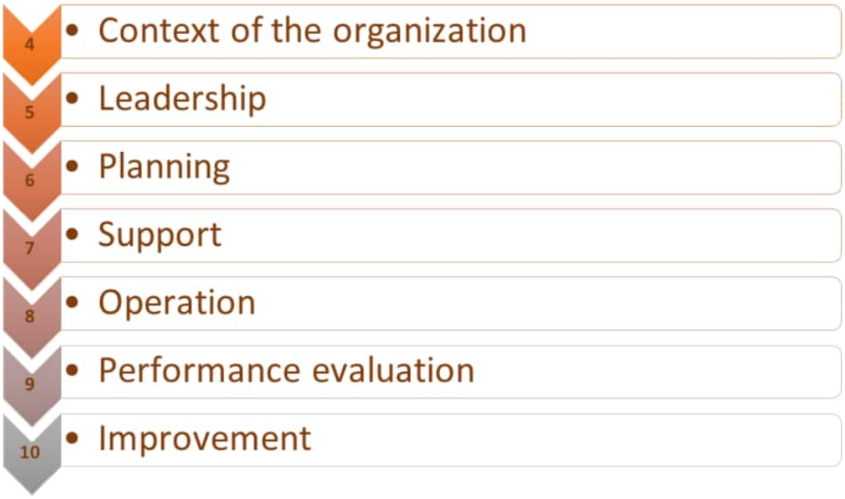
## WHAT ARE THE ISO 27001 CONTROLS?

The ISO 27001 controls (also known as safeguards) are the practices to be implemented to reduce risks to acceptable levels. Controls can be technological, organizational, physical, and human-related.

## HOW MANY CONTROLS ARE THERE IN ISO 27001?

The 2022 revision of ISO 27001 Annex A lists 93 controls organized into four sections numbered A.5 through A.8, as explained below.

Figure: ISO 27001 requirements and structure



## ISO 27001 MANDATORY DOCUMENTS

ISO 27001 specifies a minimum set of policies, plans, records, and other documented information that are needed to become compliant. Therefore, the standard requires you to write specific documents and records that are mandatory for ISO 27001 implementation and certification.

## WHAT IS "ISO 27001 CERTIFIED"?

A company can go for ISO 27001 certification by inviting an accredited certification body to perform the certification audit and, if the audit is successful, to issue the ISO 27001 certificate to the company. This certificate will mean that the company is fully compliant with the ISO 27001 standard.

An individual can go for ISO 27001 certification by going through ISO 27001 training and passing the exam. This certificate will mean that this person has acquired the appropriate skills during the course.

## AN OVERVIEW OF THE VERSIONS OF ISO 27001

As of the publication of this article, the current version of ISO 27001 is ISO/IEC 27001:2022, released in October 2022.

The first version of ISO 27001 was released in 2005 (ISO/IEC 27001:2005), and the second version in 2013. The current 2022 version is the third revision of the standard.

## IS ISO 27001 MANDATORY?

In most countries, implementation of ISO 27001 is not mandatory. However, some countries have published regulations that require certain industries to implement ISO 27001. To determine whether ISO 27001 is mandatory or not for your company, you should look for expert legal advice in the country where you operate.

Public and private organizations can specify compliance with ISO 27001 as a legal requirement in their contracts and service agreements with their suppliers.

## VACO IS HERE TO HELP

A comprehensive offering that provides businesses with customized policies and procedures designed to improve efficiency, reduce risk, and ensure compliance with legal and regulatory requirements. The service includes a review of the company's current policies and procedures, an assessment of any gaps or areas of weakness, and the development of new policies and procedures tailored to the company's specific needs. VACO's team of experts will work closely with the company to understand its unique challenges and goals, and then develop policies and procedures that address those challenges and align with best practices in the industry. The service also includes ongoing maintenance and updates to policies and procedures to ensure they remain up to date with changing UAE regulations and business needs. Find out today how you can gain the knowledge and skills needed to achieve ISO certification and enhance their performance and reputation!

# Need More?

# VACO Has You Covered

VACO Middle East is a leading consulting firm that provides innovative and customized solutions to help businesses thrive in the dynamic global market. We specialize in a range of services, including strategic planning, human resource development, accreditations, and marketing strategy development, tailored to meet the unique needs of start-ups and established companies alike. With our expertise and collaborative approach, we can help you take your business to the next level and achieve your goals. Reach out to our team today and find out how you can grow your business.

VACO
Value Add Company
واكو
Middle East Est.

**VACO Middle East Est.**
Abu Dhabi, United Arab Emirates
Visit us at www.vaco.ae
info@vaco.ae
+971 56 947 9733