27001 Academy
ISO 27001 and ISO 22301 Online Consultation Center

What is **ISO 27001** and why should you implement it?

WHITE PAPER

Advisera
Making certification simple.

Table of Contents

Executive Summary

ISO 27001 is the most important (and the most widespread) standard in the ISO 27000 series, and can be implemented in any kind of organization, profit or non-profit, private or state-owned, small or large. It enables companies to become certified, which means that an independent certification body has confirmed that an organization has implemented information security compliant with ISO 27001. As a result, ISO 27001 has become the most popular information security standard worldwide and many companies have certified against it. But because the task can be daunting, a comprehensive implementation plan often gets downgraded to one of limited scope, and company's executives may wonder, "Why would we need this standard at all?"

This white paper presents a way out from under that weight. It begins with a discussion of the logic behind this standard with the central idea of risk management and how an organization can benefit from ISO 27001's ability to protect its confidentiality, integrity and availability of the information in a company. This paper then produces a list of the most common issues ISO 27001 helps to address, where some of these issues are typical for a particular industry, while other issues are relevant for all industries. Organizations that are able to be prepared and organized in addressing the key issues specific to the business will be able to implement and certify against ISO 27001 in as short as 4 to 6 months for a small company, in up to 10 months for a mid-sized company, and in 12 months or more for a larger company. As a result, your organization can free up its IT budget for new projects that ultimately better serve the business.

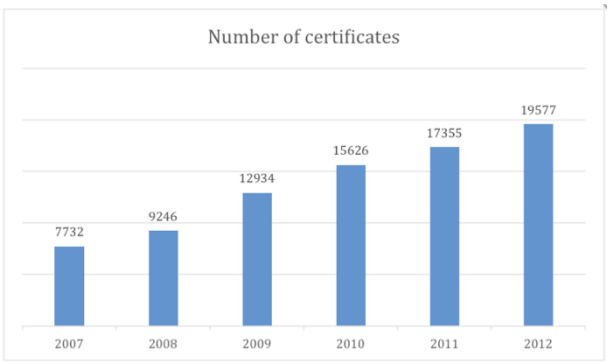
What is **ISO 27001?**

ISO 27001 is an international standard published by the International Standardization Organization (ISO), and it describes how to manage information security in a company. The latest revision of this standard was published in 2013, and its full title is now ISO/IEC 27001:2013. The first revision of the standard was published in 2005, and it was developed based on the British standard BS 7799-2.

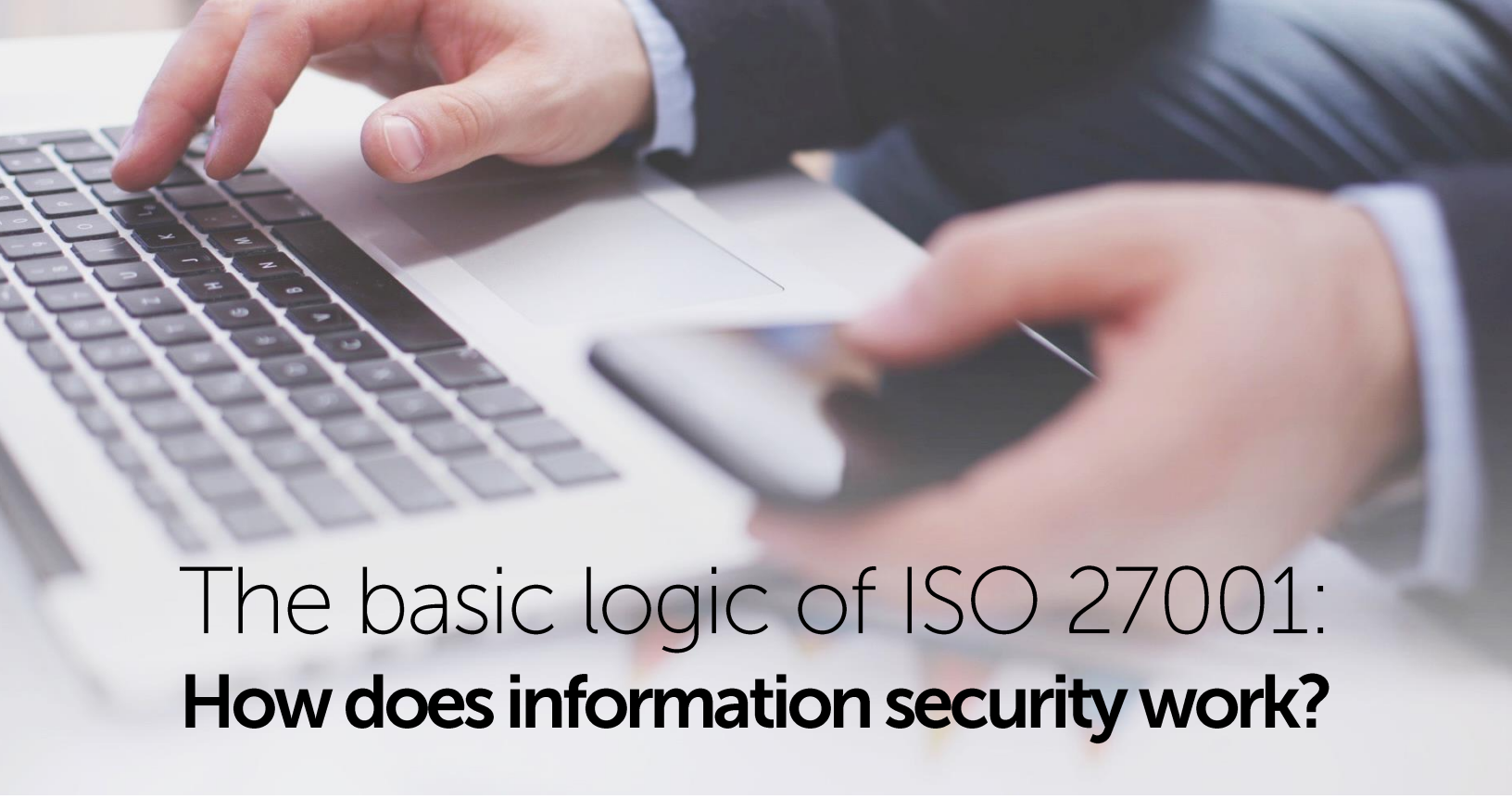
ISO 27001 can be implemented in any kind of organization, profit or non-profit, private or state-owned, small or large. It was written by the world's best experts in the field of information security and provides methodology for the implementation of information security management in an organization. It also enables companies to become certified, which means that an independent certification body has confirmed that an organization has implemented information security compliant with ISO 27001.

Currently there are ca. 40 standards in the ISO 27000 series, out of which ISO 27001 is the most important and the most widespread since this is the only information security standard against which companies can get certified.

ISO 27001 has become the most popular information security standard worldwide and many companies have certified against it – here you can see the number of certificates in the last couple of years:



Source: The ISO Survey of Management System Standard Certifications



The basic logic of ISO 27001:
How does information security work?

When speaking with someone new to ISO 27001, very often the same problem is encountered: this person thinks the standard will describe in detail everything they need to do – for example, how often they will need to perform backup, how distant their disaster recovery site should be, or even worse, which kind of technology they must use for network protection or how they have to configure the router.

Here's the bad news: ISO 27001 does not prescribe these things; it works in a completely different way. Here's why…

Let's imagine that the standard prescribes that you need to perform a backup every 24 hours – is this the right measure for you? It might be, but many companies nowadays will find this insufficient – the rate of change of their data is so quick that they need to do backup if not in real time, then at least every hour. On the other hand, there are still some companies that would find the once-a-day backup too often – their rate of change is still very slow, so performing backup so often would be overkill.

The point is – if this standard is to fit any type of a company, then this prescriptive approach is not possible. So, it is simply impossible not only to define the backup frequency, but also which technology to use, how to configure each device, etc.

By the way, this perception that ISO 27001 will prescribe everything is the biggest generator of myths about ISO 27001 – see also 5 greatest myths about ISO 27001.

Use this free "Why ISO 27001 – Awareness presentation" while preparing for the presentation of the standard.

Risk management is the central idea of ISO 27001

So, you might wonder, "Why would we need a standard that doesn't tell us anything concretely?"

Because ISO 27001 gives you a framework for you to decide on appropriate protection. The same way, e.g., you cannot copy a marketing campaign of another company to your own, this same principle is valid for information security – you need to tailor it to your specific needs.

In essence, 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 problems could happen to the information (i.e., risk assessment), and then defining what needs to be done to prevent such problems from happening (i.e., risk mitigation or risk treatment). Therefore, the main philosophy of ISO 27001 is based on managing risks: find out where the risks are, and then systematically treat them.

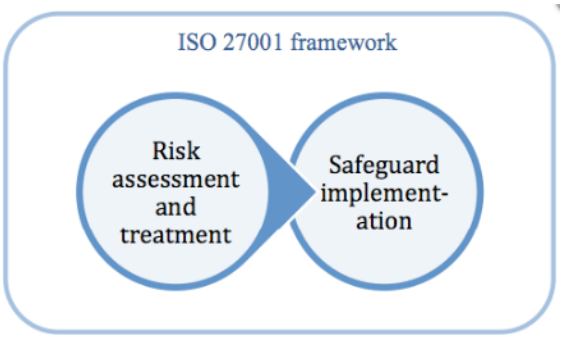


Figure: Method of safeguard selection in ISO 27001

The whole idea here is that you should implement only those safeguards (controls) that are required because of the risks, not those that someone thinks are fancy; but, this logic also means that you should implement all the controls that are required because of the risks, and that you cannot exclude some simply because you don't like them – see also: ISO 27001 risk assessment & treatment – 6 basic steps.

IT alone is not enough

If you work in the IT department, you are probably aware that most of the incidents are happening not because the computers broke down, but because the users from the business side of the organization are using the information systems in the wrong way.

And such wrongdoings cannot be prevented with technical safeguards only – what is also needed are clear policies and procedures, training and awareness, legal protection, discipline measures, etc. Real-life experience has proved that the more diverse safeguards are applied, the higher level of security is achieved.

And when you take into account that not all the sensitive information is in digital form (you probably still have papers with confidential information on them), the conclusion is that IT safeguards are not enough, and that the IT department, although very important in an information security project, cannot run this kind of project alone.

Again, this fact that IT security is only 50% of information security is recognized in ISO 27001 – this standard tells you how to run the information security implementation as a company-wide project where not only IT, but also the business side of the organization, must take part.

Getting the top management aboard

But, ISO 27001 doesn't stop with the implementation of various safeguards (help yourself to Implement ISO 27001 using this free Diagram of ISO 27001:2013 Implementation) – its authors understood perfectly well that people from the IT department, or from other lower- or mid-level positions in the organization, cannot achieve much if the executives at the top don't do something about it.

For instance, you may propose a new policy for the protection of confidential documents, but if your top management does not enforce such policy with all employees (and if they themselves do not comply with it), such a policy will never gain a foothold in your company.

So, ISO 27001 gives you a systematic checklist of what the top management must do:

- set their business expectations (objectives) for information security
- publish a policy on how to measure whether those expectations are met
- designate main responsibilities for information security
- provide enough money and human resources
- regularly review whether all the expectations were really met

This free Project proposal for ISO 27001 implementation will help you obtain support from your management.

Not allowing your system to deteriorate

If you work in a company for a couple of years or more, then you probably know how the new initiatives/projects work – at the beginning they look nice and shiny and everyone (or at least most of the people) are trying to do their best to make everything work. However, in time, the interest and the zeal deteriorate, and with them, everything related to such a project also deteriorates.

For instance, you may have had a classification policy that worked fine initially, but in time the technology changed, the organization changed and people changed, and if no one has cared to update the policy, it will become obsolete. And, as you are well aware, no one will want to comply with an obsolete document, meaning that your security will grow worse.

To prevent this, ISO 27001 has described a couple of methods that prevent such deterioration from taking place; even more, those methods are used to improve the security over time, making it even better than it was at the time when the project was at its highest. These methods include monitoring and measurement, internal audits, corrective actions, etc.

Therefore, you shouldn't be negative about ISO 27001 – it may seem vague at first reading, but it can prove to be an extremely useful framework for resolving many security problems in your company. What's more, it can help do your job more easily, and get more recognition from the top. (See also: 4 reasons why ISO 27001 is useful for techies.)

If you have implemented the 2005 revision of the standard, the "Twelve-step transition process from ISO 27001:2005 to 2013 revision" white paper will help you to migrate to the newest version.

Four **Key Benefits** of ISO 27001

Have you ever tried to convince your management to fund the implementation of information security? If you have, you probably know how it feels – they will ask you how much it costs, and if it sounds too expensive they will say no.

Actually, you shouldn't blame them – after all, their ultimate responsibility is profitability of the company. That means, their every decision is based on the balance between investment and benefit, or to put it in management's language – ROI (return on investment).

This means you have to do your homework first before trying to propose such an investment – think carefully how to present the benefits, using language the management will understand and will endorse.

In our experience, the following four are the most important benefits of ISO 27001:

COMPLIANCE

MARKETING EDGE

LOWER COSTS

BETTER ORGANIZATION

Compliance

It might seem odd to list this as the first benefit, but it often shows the quickest "return on investment" – if an organization must comply to various regulations regarding data protection, privacy and IT governance (particularly if it is a financial, health or government organization), then ISO 27001 can bring in the methodology which enables to do it in the most efficient way.

Marketing edge

In a market which is more and more competitive, it is sometimes very difficult to find something that will differentiate you in the eyes of your customers. ISO 27001 could be indeed a unique selling point, especially if you handle clients' sensitive information.

Lowering the expenses

Information security is usually considered as a cost with no obvious financial gain. However, there is financial gain if you lower your expenses caused by incidents. You probably do have interruption in service, or occasional data leakage, or disgruntled employees. Or disgruntled former employees.

The truth is, there is still no methodology and/or technology to calculate how much money you could save if you prevented such incidents. But it always sounds good if you bring such cases to management's

Organizing the business processes

This one is probably the most underrated – if your company has been growing sharply for the last few years, you might experience problems like – who has to decide what, who is responsible for certain information assets, who has to authorize access to information systems etc.

ISO 27001 is particularly good in sorting these things out – it will force you to define very precisely both the responsibilities and duties, and therefore

To conclude – **ISO 27001 could bring in many benefits besides being just another certificate on your wall**. In most cases, if you present those benefits in a clear way, the management will start listening to you.

This Project plan for ISO 27001 / ISO 22301 implementation will help you to prepare the project and its outcomes. Being organized is just one more thing that management likes.

Case study for data centers:
An interview with Goran Djoreski

Goran Djoreski is the CEO of the independent Data Center Altus Information Technology. Previously, he worked for 12 years in the financial industry, employed with Card business development, as well as the security of credit card payments. In this interview we discussed which obstacles they found while implementing ISO 27001, and how they are using this standard to compete in the market.

More than a year and a half has passed since you were certified by ISO 27001 – what are your impressions? Was it really worth it?

GD: It was definitely worth it, since it turned out that an ISO 27001 certification is not necessarily a competitive advantage, but rather a must-have. The background of the whole story is that we are trying to address the regulatory demanding markets. So we are talking about the pharmaceutical industry, telecommunications, financial industry, perhaps in the future also food production and similar, and they are all together extremely regulated, and in a conversation with them you find out that ISO 27001 is something they expect, or else they are not willing to talk to you. So one would not say it is worth it in the sense that it has brought customers to us; rather, it actually provided entry into a market we otherwise would not have had access to.

How beneficial is the ISO 27001 certificate for you as a provider of infrastructure services, if considered that this standard has a focus on information?

GD: I would say that ISO 27001 isn't based only on information, but also on everything that helps to ensure the safety and transfer of this information, and everything needed to make this information available, authentic, etc. In fact, the information as such is nothing; it cannot exist outside an infrastructure.

Is it the duty of the consultant to write your documentation or not?

GD: No. The document templates were of big help for us. Not so much because of the content, but to be able to see how this form needed to look and what topics needed to be contained with respect to the standard. Let's take the example of password policy; the very fact that we knew we had to write how we deal with passwords and that it needed to be in a specific part of the documentation helped us.

Finally, what are the 3 issues you would recommend to IT companies that only started with the ISO 27001 certificate? What do they need to pay attention to before they start with the implementation?

GD: Below are the 3 important issues considered important for IT companies to address:

They need to answer the question of why they want an ISO 27001 certificate, which means, do they want it, do they need it, and if they need it, how motivated are they to have it? This is to be done in the very beginning, giving pluses and minuses.

There must not be any dilemma at any time, since during the discussion there will often be a moment to decide how to allocate the resources between projects. If you decide that you want ISO then the management commitment must be strong, must be stronger than others that directly generate income.

Pay attention to loose ends. Like with any project, with ISO 27001 you come up with approximately 95% of everything, and then have enough of the project and the certifiers and the internal auditor who asks irrelevant questions with 20 tasks added on top just when you thought you had finished it. Then it is essential to reach the finish line, the last 5%, then everything gets easier.

Click here to read the rest of the interview…

Is ISO 27001 among **the top ISO standards?**

Do you know which ISO standards are the most popular? And whether ISO 27001 is among the most popular? There is both good and bad news for information security enthusiasts – ISO 27001 really is among the most popular, but it is insignificant compared to, say, ISO 9001.

Top ISO standards

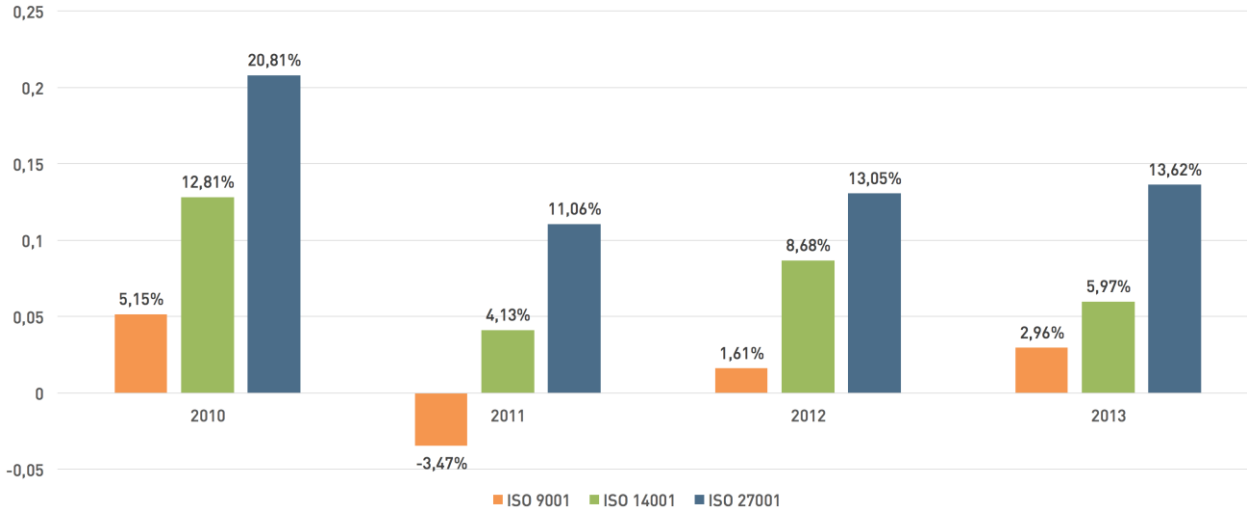
Unfortunately, there is no official data that is more current, but according to a 2011 ISO survey, these are the most popular standards worldwide:

- ISO 9001 (quality management): 1,111,698 certificates
- ISO 14001 (environmental management): 267,457 certificates
- ISO/TS 16949 (quality management for automotive-related products): 47,512 certificates
- ISO 13485 (quality management for medical devices): 20,034 certificates
- ISO 22000 (food safety management): 19,980 certificates
- ISO/IEC 27001 (information security management): 17,509 certificates

Note: this survey did not include ISO 22301, since it was published in 2012.

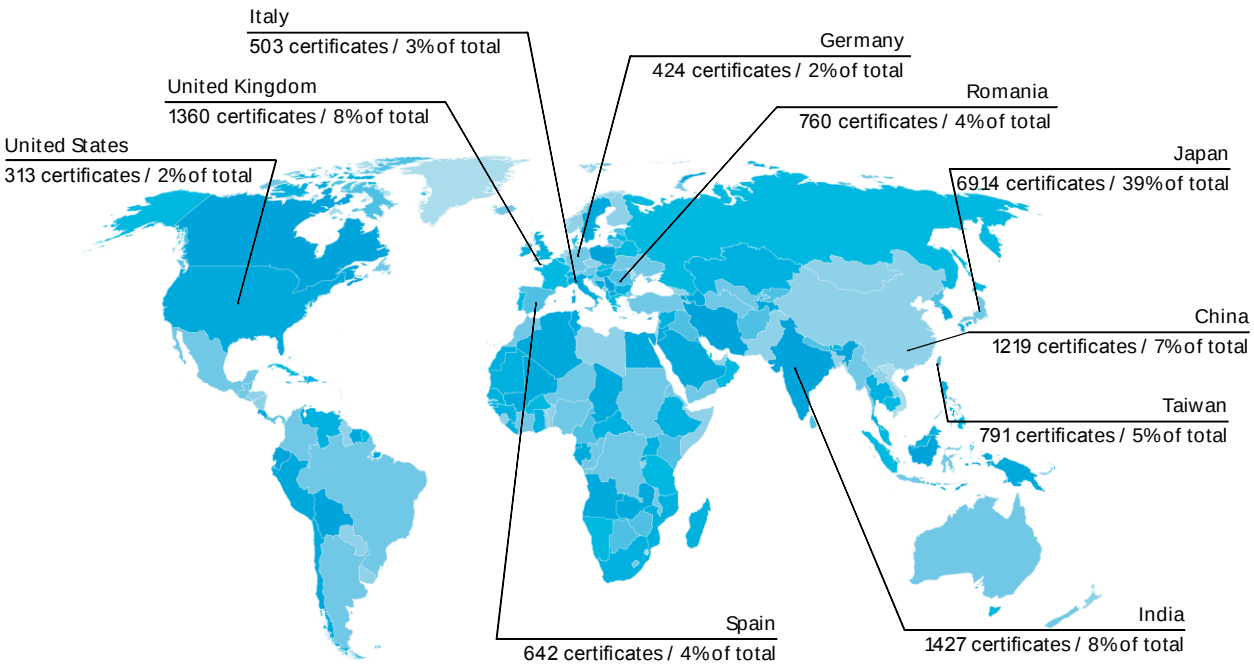
Trend looks good for ISO 27001

When we look at the trends, the situation is a bit better – ISO 27001's growth rate is among the highest, while at the same time showing the most stable growth among all the top standards (growth in % compared to previous year):



ISO 27001 by country

Since this is a very common question, let's see in which countries ISO 27001 was the most popular (in 2011):



Applicability

of ISO 27001 divided by industry

This is a list of the most common issues ISO 27001 helps to address. Some of the issues are typical for a particular industry, while other issues are relevant for all industries.

Industry	Issues to resolve	How ISO 27001 can help
All industries	Complying with a growing number of legal and regulatory requirements	ISO 27001 gives a very good framework for identifying all the requirements and defining a systematic way to comply with all of them; further, most of the information security legislation is based on ISO 27001 anyway.
All industries	Defending against a growing number of security incidents (i.e., hacker attacks, industrial espionage, embezzlements, hardware failures, etc.)	ISO 27001 provides a methodology to counter different types of threats – physical, cyber, internal, natural, etc. It is very good at merging different types of security activities into a single system.
All industries	Prioritizing investments in security	By assessing risks according to ISO 27001, you will have a clear picture of which safeguards must be implemented quickly.
All industries	Decreasing the cost of security incidents	The basic logic of ISO 27001 is to try to prevent incidents – in most cases, the cost of ISO 27001 implementation is much lower than the cost savings achieved because of incidents that were prevented.

Industry	Issues to resolve	How ISO 27001 can help
All industries	Providing a tool for top management with which they can understand and control security issues	ISO 27001 has several sections dedicated to top management – how it has to be involved in managing information security, and which information it has to receive. Best of all is that ISO 27001 helps information security professionals start presenting their work in business language, which is the language understood by top executives.
All industries	Gaining competitive advantage in tenders	Many large companies, financial organizations, and government agencies prefer suppliers who are ISO 27001 certified.
All industries	Defining security roles and responsibilities	ISO 27001 requires clear definition of who is responsible for what related to security; it also provides a natural way of identifying who should be responsible for which area.
IT companies (cloud providers, software developers, etc.)	Convincing customers their information is safe	By obtaining an ISO 27001 certificate, companies provide proof (issued by a certification body) that they protect the information in accordance with the leading information security standard.
Various service providers (online and offline)	Decreasing the penalties due to unavailability of their service	Implementation of ISO 27001 increases the level of resilience of an organization – as a consequence, the number of incidents is lower, and their duration is shorter.
Financial institutions	Finding the methodology for managing operational risk	Managing information security risks is part of the operational risk management; therefore, ISO 27001 provides a methodology for managing a larger part of operational risks.
Health organizations	Protecting the health records	ISO 27001 provides a methodology for protection of all kind of information – especially the information that is considered the most sensitive (e.g., customer or patient personal data).
High-tech companies	Protection of intellectual property	ISO 27001 provides a methodology for protection of all kind of information – especially the information that is considered the most sensitive (e.g., know-how, product development, etc.).
Consulting companies	Finding the methodology to help resolve their clients' security issues	ISO 27001 provides step-by-step flow for consulting companies to implement information security safeguards in their clients' companies.

Conclusion

ISO 27001 will most probably continue its high growth, especially due to cybersecurity threats and an ever-growing reliance on information technology. Having an information management security system that is ISO 27001 compliant helps to communicate to business partners and clients that your company is seriously committed to information security and makes a credibility statement that controls are in place without having to reveal confidential security processes.

While it is unlikely to become as popular as ISO 9001, as more companies require the certification as a requirement for doing business, our guess is it will probably reach 3rd position (immediately behind ISO 9001 and ISO 14001) in the next couple of years, and expected to hold this position for the years to come.

To learn about the wider context of information security, read this free e-book "9 Steps to Cybersecurity" that will help you to understand cybersecurity basics in an easy-to-digest format.

References

27001 Academy: http://www.advisera.com/27001academy

Wikipedia - ISO/IEC 27001:2013: http://en.wikipedia.org/wiki/ISO/IEC_27001:2013

ISO 27001 Security: http://www.iso27001security.com

27001 Academy

ISO 27001 and ISO 22301 Online Consultation Center

EPPS Services Ltd.
for electronic business and business consulting
Ul. Vladimira Nazora 59, 10000 Zagreb
Croatia, European Union

Email: support@advisera.com
Phone: +1 (646) 759 9933
Toll-Free (U.S. and Canada): 1-888-553-2256
Toll-Free (United Kingdom): 0800 808 5485
Fax: +385 1 556 0711

EXPLORE THE ACADEMIES

9001 Academy | 14001 Academy | 18001 Academy | 20000 Academy

Advisera

Making certification simple.