From a Series of e-Books published by deGRANDSON Global

THE FAQS ABOUT ISO 27001

The ISO Standard for Information Security Management Systems (ISMS)

From deGRANDSON Global – the e-Learning Company

October 2023

Contents

The ISO 27001 Standard 4

What is ISO? 4

What does ISO 27001 mean? 5

What is the purpose of ISO 27001? 6

What is an Information Security Management System (ISMS)? 7

What is the Purpose of an Information Security Management System? 8

Who needs an Information Security Management System? 9

What are the benefits of a formal Information Security Management System? 10

Certification to ISO 27001 13

What is ISO 27001 Certification? 13

Do You Need ISO 27001 Certification? 14

Who can benefit from ISO 27001 Certification? 15

What are the Benefits of Having ISO 9001 Certification? 16

How much does ISO 27001 Certification Cost? 17

Who Issues ISO 27001 Certification? 19

How to Get an ISO 27001 Certificate? 20

Are the Controls listed in Annex A, Statement of Applicability, enough to meet requirements? 21

Why are there so many Standards (47+) in the ISO 27000 Series of Standards? 22

What is the significance of ISO 27002? 23

Where do other established IS Standards like PCI-DSS or the Payment Card Industry Data Security Standard fit in? 24

Can I get Certified to ISO 27701, Personal Information? 25

Can we get one site Certified to ISO 27001, or must it be the entire organization? 26

Is GDPR Compliance compatible with ISO 27001 Certification? 27
We're an SME. Do we need cybersecurity? 28
How to Choose a Certification Body? 29
Are £1995 ISO 27001 Certificates You Can Get Within 30 Days Legitimate? 30
Why is it Important to Get Certified by the Proper Certification Body? 31
How does the ISO 27001 Certification Process Go? 32
How to check the ISO 27001 Certification of an organization? 34
Do Management Representatives or others responsible for an ISMS need training? 35
Do Internal Auditors need training? 36
Got a question we haven't answered? 37

The Author:

Dr John FitzGerald

Director and founder of deGRANDSON Global. After 15 years in manufacturing industry, John has spent the past 25 years training, consulting, and auditing ISO 9001, ISO 14001, ISO 13485, ISO 27001, ISO 45001, ISO 17025, and other management systems. 'Our objective is to be a world-class provider of e-training using the best-proven technology to satisfy and, hopefully, delight all of our Learners. Great commercial success and professional esteem will surely follow.' Please find me on Facebook and LinkedIn.

The ISO 27001 Standard

What is ISO?

The International Organization for Standardization (ISO for short) is the world's largest developer of voluntary International Standards. Their 21,000+ standards offer solutions and best practice guidance for all types of technology and businesses, helping companies and organizations increase performance while protecting consumers and the planet.

While most are product and technical standards, the ISO has developed 40+ management system standards.

The best known of these include ISO 9001 (quality), ISO 14001 (environment), ISO 45001 (health & safety) and ISO 27001 (information security management). The feature they all have in common is that they are auditable. They are written to facilitate auditing by an independent third party (e.g., CAB) to confirm compliance with the standards' requirements.

ISO 13485 is a quality management system standard based on ISO 9001, considered the parent of all the other standards.

For more, visit ISO 9001 on the ISO website.

Enjoy!

What does ISO 27001 mean?

ISO 27001 (or, to give it its full title, ISO 27001:2022, Information Technology - Security Techniques - Information Security Management Systems — Requirements) is an internationally recognized standard that sets out the requirements for an Information Security Management System (ISMS).

It was initially developed by the British Standards Institute and known as BS 7799. It became an international standard in 2000 as ISO/IEC 17799, "Information Technology - Code of Practice for Information Security Management' when published under the auspices of the International Standards Organization (ISO). This Guide was incorporated into the ISO 27000 Series in 2005 as the Code of Practice, ISO 27002.

ISO 27001 was first published in 2005 and later replaced by a second version, ISO 27001:2013. The current version was issued in 2022 and remains the current version.

As every organization has information of value and **every organization, especially the SMEs seen to be a soft target and route into major organizations' networks, is a target for crypto-criminals**, ISO 27001 is relevant and globally applicable to all kinds of organizations.

What is the purpose of ISO 27001?

The purpose of the Standard is to provide a framework for an organization to develop a management system that will **control the risks associated with information and data to a high level of confidence.**

Note carefully that this Standard does not deal with Information Technology (computerized data) alone. Data in all shapes and forms and the physical resources (the premises) used to protect them are included.

The Standard requires that management:

- Systematically examine the organization's information security risks, taking account of the threats, vulnerabilities, and impacts (PLAN);
- Design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable (DO) and
- Adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis (CHECK & ACT).

What is an Information Security Management System (ISMS)?

An **ISMS** is a systematic and formal approach consisting of processes, technology, **and people** that enables an organization **to protect and manage its information assets, physical and virtual,** through effective risk management.

What is the Purpose of an Information Security Management System?

An ISMS helps coordinate and direct an organization's attention to assuring the adequacy of controls against information security threats and, using Annex A of the Standard, to ensure that all commonplace vulnerabilities have been addressed.

Who needs an Information Security Management System?

Whether you realize it or not, you already have an informal ISMS. You back up your computer data, don't you? You ensure that strangers can't enter and walk about your premises.

Do you check the backgrounds of potential recruits before you employ them? And so on. You have many information security controls already in place.

But the critical question is, are your current IS Controls enough to prevent all but the most technically advanced crypto criminals from breaching your cyber defenses?

You are most unlikely to be adequately protected without applying the rigorous requirements of ISO 27001 and applicable supplements. Just think for a moment about what you would do if you arrived at work tomorrow morning to find a ransom demand on every screen, all your data encrypted, and unless you pay up immediately, you're out of business.

What are the benefits of a formal Information Security Management System?

There are at least twenty benefits that organizations with a quality management system in place can enjoy, such as:

1. **Recognized reputation as a security-conscious organization.** Even more, you have an internationally recognized certificate to prove it,

2. **Awareness at all levels and functions within the organization.** As an organization, you must always be prepared for the existential threat that data theft poses (e.g., through phishing) for the business and for their individual responsibility in protecting that information.

3. **Awareness that information security is about protecting physical assets.** This awareness covers practices in the workplace, personal behavior, working from home, etc., and not just about computer systems.

4. **Satisfaction at the Board level.** Members of the organization can rest assured that information assets are being properly cared for,

5. **Satisfaction for Suppliers and Customers.** Both suppliers and customers can be reassured that their information assets and/or intellectual property is being professionally protected (your customers will be aware that attack through their Suppliers' ICT systems is a well-known vulnerability),

6. **Objective evidence for Senior Management, the C-Suite.** With the help of independent auditing, senior management can be assured that information security policies are being adequately implemented,

7. **The reassurance that Information Security processes are in place.** This will help ensure that the organization learns from its mistakes and that such errors and breaches occur only once,

8. **Reduced risk of data loss and reputational damage.** This can be achieved by having a robust and tested ISMS implemented and maintained that is suited to the vulnerabilities and threats the business faces,

9. **A larger pool of** qualified candidates **applying to work with your business.** Attracting top talents to your organization is much easier when you have an excellent reputation.

10. **Reduced absenteeism and employee turnover rates.** Employees have objective reasons to feel secure in their jobs and to value them,

11. **Improved ability to respond to regulatory compliance issues.** With an enhanced relationship with GDPR and other personal data regulatory authorities, you don't have to be on edge whenever new rules or guidelines get announced.

12. **Reduced cost of security incidents.** You have a system in place to investigate them and to take formal action to prevent their recurrence,

13. **Reduced downtime and the costs of disruption to operations.** Thanks to fewer information security incidents, issues can be dealt with systematically and efficiently,

14. **Reduced cost of insurance premiums.** This is because insurance companies recognize that certified businesses make fewer and less costly claims,

15. **Peer recognition for having achieved an international benchmark.** This, in turn, influences current and potential customers who are concerned about their intellectual property security,

16. **Improved scoring in pre-tender documents.** This helps ensure that your organization gets a chance to compete with established businesses (especially true for public sector organizations),

17. **Reduced fines if prosecuted.** Your Certification constitutes objective evidence to a court of the seriousness with which information security is treated,

18. **Improved Management control.** This covers all forms of business data and information,

19. **A formalized approach to continual improvement.** When it comes to information security performance, consistency is vital.

20. **Continual review of the ISMS.** Ensuring that the ISMS is aligned with the business's strategic plan is essential.

For more, visit ISO 27001 and the Manufacturing and Service Industry.

Certification to ISO 27001

What is ISO 27001 Certification?

An ISO 27001 Certificate is recognition from a Certification Body – CAB (usually an accredited Certification Body) that an organization has implemented and is maintaining an information security management system that meets the requirements of ISO 27001:2022.

Do You Need ISO 27001 Certification?

Yes and No.

In many cases, ISO 27001 Certification is not mandatory. Still, it can be a useful tool to add credibility by demonstrating that you manage business information securely suited to your customers' expectations. For some industries, Certification is a legal or contractual requirement. An SLA - Service Level Agreement will specify information security requirements in other cases.

Who can benefit from ISO 27001 Certification?

Organizations globally, both public and private spheres, and from every economic sector, can benefit from maintaining an ISO 27001-compliant Information Security Management System (ISMS) for your entire supply chain.

What are the Benefits of Having ISO 9001 Certification?

In terms of information security, an ISMS allows an organization to:

1. Satisfy the security requirements of customers and other stakeholders.
2. Improve an organization's plans and activities.
3. Meet the organization's information security objectives.
4. Comply with regulations, legislation, and industry mandates; and
5. Manage information assets in an organized way that facilitates continual improvement and adjustment to current organizational goals and the environment.

Furthermore, the independent Certification involved in ISO 27001 Certification will permit an organization to:

1. Achieve greater assurance that its information assets are adequately protected against information security risks on a continual basis.
2. Maintain a structured and comprehensive framework for identifying and assessing information security risks, selecting and applying applicable controls, and measuring and improving their effectiveness.
3. Continually improve its control environment; and,
4. Effectively achieve legal and regulatory compliance.
5. Management performance improved as less time is spent apologizing to customers and managing the unnecessary repetition of work.

How much does ISO 27001 Certification Cost?

The cost of ISO 27001 certification varies hugely based on the organization's size, geographical location, and economic prosperity.

Let's take the example of an SME with ten employees. Here are some typical prices from the UK for 2023, where we consider three scenarios …

Scenario (1)	Do-it-yourself (2)	Minimum Consultancy Support (3)	Maximum Consultancy Support (4)
Develop ISMS (8 days)	£800	£1600	£4000
Implement ISMS (8 days)	£800	£1600	£4000
Maintain ISMS (2 x 3 years)	£600	£600	£3000
Certification Year 1	£2500	£2500	£2500
Year 2	£1000	£1000	£1000
Year 3	£1000	£1000	£1000
Total 3-year cost	**£6700**	**£8300**	**£15500**
Typical duration to Certification	11 months	5 months	4 months

Notes:

1. It is necessary to examine a 3-year horizon as CABs play games with their quotations that can be confusing. What is a given, however, is that CAB Audits and the associated contract must, under IAF rules, be based on a 3-year cycle.
2. No outside help. The project leader would need ISO 27001 Lead Implementer Training.
3. Four days of consultancy support are included here. Priced at £ 500 p.d., consultancy costs range from £300 to £700 per day. Satisfactory references must be obtained for previous ISO 9001 projects.

4. Maintenance here includes two days annually for internal auditing and Management Review support.

The best advice for controlling costs is to shop around and recheck the competitiveness of your chosen CAB regularly.
For more, visit the ISO 27001 Lead Implementer Certification Course. Also, see 31 steps to ISO 27001 Certification.

Who Issues ISO 27001 Certification?

The ISO develops International Standards, such as ISO 9001 and ISO 14001, but is not involved in their Certification. It does not issue certificates. ISO 27001 certification is performed by external certification bodies; so **a company or organization cannot be certified by the ISO organization itself**.

How to Get an ISO 27001 Certificate?

Certificates are issued by CABs after they have gone through an ISO Certification process. This process is based on a comprehensive 2-stage audit (itself based on the auditing standard, ISO 19011), which involves a documentation review and an independent on-site audit.

The CAB gathers and documents objective evidence of compliance with the requirements of ISO 27001. After the CAB has confirmed that all the requirements of the Standard have been implemented and are being maintained, a Certificate is issued as is permission to use logos to publicize the fact.

For more, visit IAF Scope regarding ISO 27001

Are the Controls listed in Annex A, Statement of Applicability, enough to meet requirements?

A Control is a precaution to reduce the risk associated with a particular vulnerability. Annex A of the Standard lists 93 vulnerabilities in 4 domains and, against each one, includes one Control. This structure has often been taken to mean that these are the only vulnerabilities to be considered and that, should a vulnerability give rise to a threat (i.e., the vulnerability applies to the organization and hence there is a threat to be managed), one Control is enough. This is not the case as ...

1. Many organizations will have IS vulnerabilities/threats unique to their business, and these will need risk assessment and risk treatment (i.e., additional Controls) and
2. One Control may not be sufficient to reduce the risk associated with a particular vulnerability/threat to an acceptably low level.

For more, see Risk Management - the Swiss Cheese Model explained.

Why are there so many Standards (47+) in the ISO 27000 Series of Standards?

Let's start with another question: Is Compliance with Other Standards and Guides in the ISO 27000 Series Mandatory?

The answer is No and Yes!

NO: There is nothing in the standards and guides making their use obligatory, but:

YES: External auditors are aware of these standards and guides and will be informally using them to frame their interview questions.

For example, suppose an organization has Personally Identifiable Information. In that case, the external auditors will ask how the organization has addressed the typical vulnerabilities identified in ISO 27701 - this is 'low-hanging fruit' for the auditor.

So, you cannot afford to ignore the Standard, and your risk assessment (and opportunities) needs to add relevant vulnerabilities from ISO 27701 to those from the Statement of Applicability in Annex A of ISO 27001.

You will need to consider all 47 Standards to decide whether they apply to your ISMS (and don't worry, as it's unlikely that more than one or two of them apply); you should visit ...

1. The chart with an overview of the ISO 27001 Series at To select your ISO 27001 Auditor Course and
2. The section What comprises the ISO 27001 Series of Standards.

What is the significance of ISO 27002?

To give it its full title, ISO/IEC 27002:2022 Information Technology — Security techniques — Code of practice for information security controls, provides guidelines for organizational information security standards and information security management practices, including the selection, implementation, and management of Controls taking into consideration the organization's information security risk environment.

It is designed to be used by organizations that intend to:

- select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001;
- implement commonly accepted information security controls;
- develop their own information security management guidelines.

You should expect External Auditors to ask whether you've used this Guide.

Where do other established IS Standards like PCI-DSS or the Payment Card Industry Data Security Standard fit in?

Many data security standards other than ISO 27001, like PCI-DSS and COBIT, remain in everyday use. Where Certification to ISO 27001 and one or more of the other Standards are needed, a single ISMS addressing all the requirements is the norm. Care needs to be taken to ensure that internal audits include the audit of all applicable requirements.

For more, see Information Security Standards other than ISO 27001.

Can I get Certified to ISO 27701, Personal Information?

The short answer is no. This is because ISO 27701, which deals with PII - Personally Identifiable Information, is **not an auditable standard**. It was published as a Supplement to ISO 27001. Its incorporation into an ISO 27001-compliant ISMS is in the form of additional Vulnerabilities/threats (as listed in ISO 27701). as applicable.

For more information, see ISO 27701 brings ISO 27000 Standards Series to a total of 47.

Can we get one site Certified to ISO 27001, or must it be the entire organization?

Certainly, an organization with multiple sites may have a single site certified to ISO 27001. However, the exchange of information between the site in question and the other sites of the organization will have to be controlled. And this is to a level that compares equally with the controls applied to information exchange with Customers and Suppliers.

Is GDPR Compliance compatible with ISO 27001 Certification?

After the release of our ISO 27001 Course on implementing an Information Security Management System (ISMS), we were asked for advice regarding the relationship between GDPR documentation and ISO 27001 documentation. There are three basic options (or strategies) to choose from when documenting GDPR and ISO 27001 compliance, namely:

1. Keep the GDPR documentation entirely separate from the ISMS and its documents,
2. Fully integrate the regulatory requirements into your ISMS Documents or
3. Keep GDPR Documents separate from **and** cross-referenced to ISMS Documents.

For more, see GDPR, ISO 27701 and ISO 27001: a natural combination?

We're an SME. Do we need cybersecurity?

As an SME, you are a particularly attractive proposition for a cyber attack. This is because cyber-criminals expect your IS Controls to be weak and, consequently, vulnerable. While they may be interested in a ransom attack, it is equally likely that they are trying to use your IT System as a back door into the systems of your major public and private sector Customers and Suppliers. That is, you are going to be their Trojan Horse!

As your Customers and Suppliers become more aware of IS, you can expect to be challenged more frequently on your information security arrangements and for these also to feature in SLAs. Your best option is to get certified to ISO 27001 sooner rather than later.

How to Choose a Certification Body?

The choice of CAB is important. An accredited CAB (e.g., BSI) should be used wherever possible, and with ISO 27001, one won't be too difficult to find.

Accreditation, issued by a nationally recognized Accreditation Board (e.g., UKAS), is an important confirmation of the legitimacy of the CAB. To help ensure an international 'level playing field' for CAB auditing standards, National Accreditation Boards have their own international organization, the International Accreditation Forum (IAF), which oversees an ongoing program of witnessed self-assessment of IAF Members of each others' activities.

A Certificate from an accredited CAB will carry three logos. #1 the CAB's own logo, #2 the Accreditation Boards logo, and #3 the IAF logo. If you present an ISO 27001 Certificate to a customer or potential customer that does not carry all three logos, expect to be challenged. Without a plausible explanation, you can expect your approach to be rejected.

Are £1995 ISO 27001 Certificates You Can Get Within 30 Days Legitimate?

Legally speaking? Yes. But the Certificate is worthless. There are 'cowboy' CABs (whom you should ask to explain how an organization can create 3 months of records, the minimum needed to prove maintenance of an ISMS, in 7 days) and even 'cowboy' Accreditation Bodies.

With ISO 27001 Certificates, making sure you have the real thing fundamentally means choosing a CAB that will get you an IAF logo for your Certificate. Ask about it by name and accept nothing else.

Why is it Important to Get Certified by the Proper Certification Body?

Remember that those reviewing tender documents are unlikely to be inexperienced. They will recognize a phony Certification instantly. And your offering will go directly into the rubbish bin with the hard work you've expended to develop products and services you are proud of totally wasted. Most importantly, you wouldn't want an ISO Auditor to find such bogus Certificates when checking your evaluation of external providers (suppliers).

For more, visit Is IAF Accreditation possible for all ISO Standards? and Your Accreditation Body must follow IAF Guidance.

How does the ISO 27001 Certification Process Go?

As you will have seen in the cost data above, there are two stages in securing ISO 27001 Certification:

Stage 1. Develop, implement, and maintain a suitable ISMS for your organization, which includes Controls for Annex A and other vulnerabilities/threats and

Stage 2. Engage the services of a CAB to undertake the necessary evaluations and ISO Certification Audits.

Stage 1. Develop, implement, and maintain a suitable ISMS for your organization:

Our Infographic shown here nicely illustrates the multi-step process of preparing for Certification (click on the infographic image to get a copy for yourself). Whichever of the three approaches you choose (or variants thereof), you will benefit from our ISO 27001 Lead Implementer Course in managing and directing your ISO 9001 Project.

Stage 2. Engage the services of a CAB to undertake the necessary evaluations and audits:

When choosing a certification body, you should:

- Evaluate several certification bodies.
- Check if the certification body auditing activities include ISO 27001:2022.
- Check if it is accredited. Accreditation is not compulsory, and non-accreditation does not necessarily mean it is not reputable, but it does provide independent confirmation of competence. To find an accredited certification body, contact the national accreditation body in your country or visit the International Accreditation Forum.

Note: the terms certification and accreditation cannot be used interchangeably, though it is not uncommon to do so. The differences between Certification and Accreditation are as follows:

Certification – the provision by an independent body of written assurance (a certificate) that the product, service, or system in question meets specific requirements.

Accreditation – the formal recognition by an independent body, generally known as an accreditation body, that a certification body operates according to international standards.

For more, visit the International Accreditation Forum/about us/ and 10 Reasons to change your ISO Certification Body.

How to check the ISO 27001 Certification of an organization?

The IAF, after struggling with the issue for many years, launched IAF CertSearch. This is an exclusive global database for accredited management system certifications. Other databases, irrespective of the organization publishing them, should be treated with skepticism or, better still, ignored.

Currently, CertSearch has over 400,000 valid certifications across more than 150 economies covering a range of sectors, 4,000 certification bodies, and 68 IAF MLA signatory accreditation bodies. While highly dependable, this database is a long way from being complete when one considers that there are 1 million plus organizations certified to ISO 9001:2015 alone. And to date, not many CABs have added their ISO 27001 customers to the Register.

Businesses and governments can digitally validate an organization's Certification (s) to determine if a certificate is valid and if the Certification Body issuing the Certificate is accredited to issue certifications to that Standard.

The direct route is, of course, always open to you – ask the organization for a copy of their current Certificate. Many will have their Certificate on display on their website.

For more, visit IAF CertSearch.

Do Management Representatives or others responsible for an ISMS need training?

The training of a Management Representative or others with day-to-day responsibility to maintain an ISMS is NOT mandatory. Training is implied as part of developing competence but not a specific stand-alone requirement. So, unless you are determined to outsource this support indefinitely (technically, that's not permitted), you need to train your Management Representative. And you're in luck. We've got exactly the Course you need.

For more, visit the ISO 27001 Lead Implementer Course.

Do Internal Auditors need training?

Again, training here is not mandatory. However, effective internal audits are essential to doing a professional job in maintaining your QMS and avoiding nasty surprises at your next Certification Body audit. Also, if you don't train them, your auditors won't have any of the skills necessary to 'harvest' those improvement suggestions from the people in your organization who actually do the work.

For more, visit the ISO 27001 Internal Auditor Course.

Got a question we haven't answered?

We'd love to hear it and, if possible, answer it for you. Just use our Support Ticket System. You'll find a Knowledge Base there that might have an immediate answer for you. Otherwise, fill in a Ticket.

For more, visit deGRANDSON Support Ticket.

deGRANDSON Global

e-Training Company