Cyber
Framework
Solutions

ISO 27001 Information Security Management System

Info@cyberframeworksolutions.com
https://www.cyberframeworksolutions.com

INTRODUCTION

ISO27001:2022 Information Security Management System Your Guide To Implementation. Inspiring trust for a more resilient world.

Data and connectivity are accelerating the extraordinary transformation of organisations, from the establishment of digital ecosystems to the optimisation of supply chains and operational procedures. But with every technological advancement, cyber-attacks, data breaches, and other operational disruptions become inevitable.
That is why organisations need to build resilience around their information security management with an internationally recognised framework like ISO/IEC 27001. ISO/IEC 27001 helps organisations show their stakeholders that they prioritize safety, privacy, reliability, cyber security, and data ethics throughout their organisation, and that their information management system is aligned with global best practice.

At Cyber Framework Solutions, we have the experience, expertise, and support services to help you get the most from ISO/IEC 27001 and make your organisation more resilient and responsive to threats. This guide shows you how to implement ISO/IEC 27001, enabling your organisation to demonstrate its commitment to information security and safeguarding its reputation with clients, suppliers, and partners in an increasingly competitive digital world. We also highlight our additional support services, which help you not only achieve certification, but continue to reduce risk and protect your business.

CFS

How ISO 27001 Works.

The ability to manage information safely and securely has never been more important. ISO/IEC 27001 not only helps protect your business, but it also protects your reputation. This standard sends a clear signal to customers, suppliers, and the marketplace that your organisation can handle information securely. ISO/IEC 27001 is a robust framework that helps you protect information such as financial data, intellectual property, or sensitive customer information. It helps you identify risks and puts in place security measures that are right for your business, as well as giving you the ability to continually review and refine the way you do this, not only for today, but also for the future.

"That's not all."

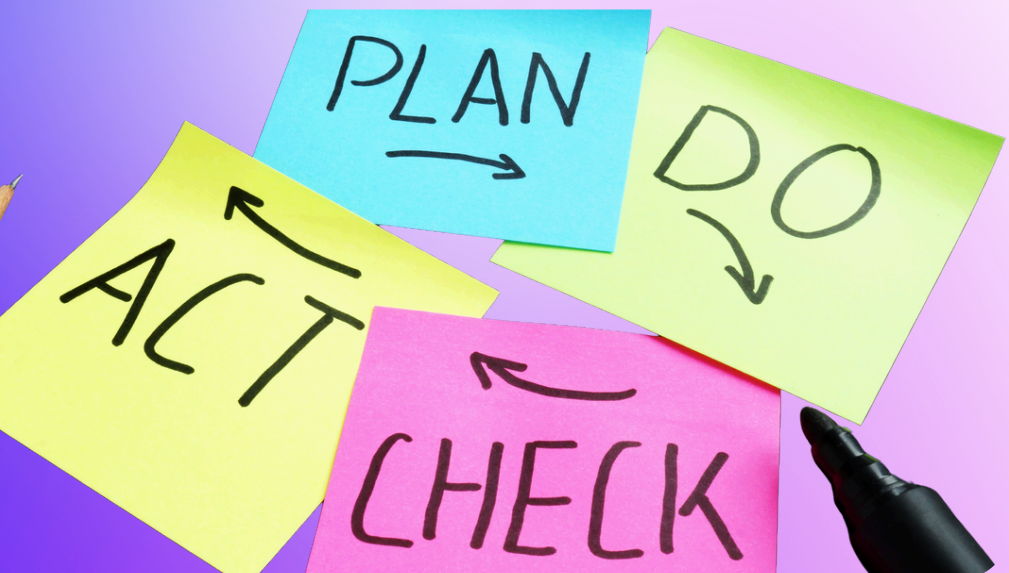
ISO/IEC 27001 lays the foundation from which you can build and strengthen digital trust across your entire digital ecosystem. It helps you effectively implement a range of complementary standards and solutions that enhance your information security practices, such as ISO/IEC 27002 (Information Security Controls) and ISO/IEC 27701 (Privacy Information Management.

CFS

PLAN,DO,CHECK,ACT MODEL (PDCA)

The approach underlying a management system for quality in healthcare organisation is based on the concept of Plan-Do-Check-Act (PDCA).
The PDCA model provides an iterative process used by organisations to achieve continual improvement through cycles of ongoing measurement of performance and assessment of changes. It can be applied to a management system for Occupational Healthcare and Safety in organisations and is briefly described as follows.

- Plan: establish healthcare quality objectives and processes necessary to deliver results in accordance with the organisation's healthcare quality policy (Clause 6).
- Do: implement the processes as planned (Clauses 7 and 8).
- Check: monitor, measure and assess processes against the organisation's policies, including its commitments, objectives and operating criteria and report the results (Clause 9).
- Act: take actions to continually improve (Clause 10).



CFS

Key Deliverables

- ISMS Scope & Statement of Applicability
  - Defines boundaries and applicability of controls.
- Information Security Policy
  - Sets the strategic direction and commitment to security.
- Risk Assessment & Treatment Plan
  - Identifies, evaluates, and mitigates risks with documented decisions.
- Asset Inventory & Classification
  - Catalogues critical assets and their protection levels.
- Annex A Control Implementation
  - Evidence of applying relevant controls across organisational, technical, physical, and human domains.
- Internal Audit Reports
  - Validates ISMS effectiveness and readiness for certification.
- Training & Awareness Records
  - Demonstrates staff competence and engagement.
- Incident Management & Corrective Actions
  - Logs, responses, and lessons learned from security events.
- Performance Metrics & Monitoring Logs
  - Tracks control effectiveness and compliance.
- Management Review Minutes
  - Shows leadership oversight and continual improvement.

CFS

ISO/IEC 27001:2022 CLAUSES

Clause 1: Scope

The first clause details the scope of the standard.

Clause 2: Normative references

All the normative references are contained in ISO/ IEC 27000, Information technology – Security techniques – Information security management systems – Overview and vocabulary, which is referenced and provides valuable guidance.

Clause 3: Terms and Definitions

Please refer to the terms and definitions contained in ISO/IEC 27000. This is an important document to read.

Clause 4: Context of the Organization

This is the clause that establishes the context of the organisation and the effects on the ISMS. Much of the rest of the standard relates to this clause. The starting point is to identify all external and internal issues relevant to your organisation and your information or information that is entrusted to you by 3rd parties. Then you need to establish all “interested parties” and stakeholders as well as how they are relevant to the information. You will need to identify requirements for interested parties which could include legal, regulatory and/or contractual obligations. You will also need to consider important topics such as any market assurance and governance goals. You will be required to decide on the scope of your ISMS, which needs to link with the strategic direction of your organisation, core objectives and the requirements of interested parties. Finally, you will need to show how you establish, implement, maintain, and continually improve the ISMS (including the processes needed and their interactions) in relation to the standard. .

CFS

Clause 5: Leadership

This clause is all about the role of “top management, ” which is the group of people who direct and control your organisation at the highest level. They will need to demonstrate leadership and commitment by leading from the top. Top management need to establish the ISMS and information security policy, ensuring it is compatible with the strategic direction of the organisation. They also need to make sure that these are made available, communicated, maintained, and understood by all parties. Top management must ensure that the ISMS is continually improved, and that direction and support are given. They can assign ISMS relevant responsibilities and authorities, but ultimately, they remain accountable for it

Clause 6: Planning

This clause outlines how an organisation plans actions to address risks and opportunities to information. It focuses on how an organisation deals with information security risk and needs to be proportionate to the potential impact they have. ISO 31000, the international standard for risk management, contains valuable guidance. Organisations are also required to produce a “Statement of Applicability” (SoA). The SoA provides a summary of the decisions an organisation has taken regarding risk treatment, the controls you have included, and those you have excluded and why you have decided to include and exclude the controls in the SOA. Another key area of this clause is the need to establish information security objectives and the standard defines the properties that information security objectives must have. Finally, this clause requires an organisation to perform changes to the ISMS in a planner manner.

CFS

Clause 7: Support

This section of ISO/IEC 27001 is all about getting the right resources, the right people, and the right infrastructure in place to establish, implement, maintain, and continually improve the ISMS. It deals with requirements for competence, awareness, and communications to support the ISMS and it could include making training and personnel available, for example. This clause also requires all personnel working under an organisation's control to be aware of the information security policy, how they contribute to its effectiveness and the implications of not conforming. The organisation also needs to ensure that internal and external communications relevant to information security and the ISMS are appropriately communicated. This includes identifying what needs to be communicated, to whom, when and how this is delivered. It is in this clause that the term "documented information" is referenced. Organisations need to determine the level of documented information that is necessary to control the ISMS. There is also an emphasis on controlling access to documented information, which reflects the importance of information security.

Clause 8: Operation

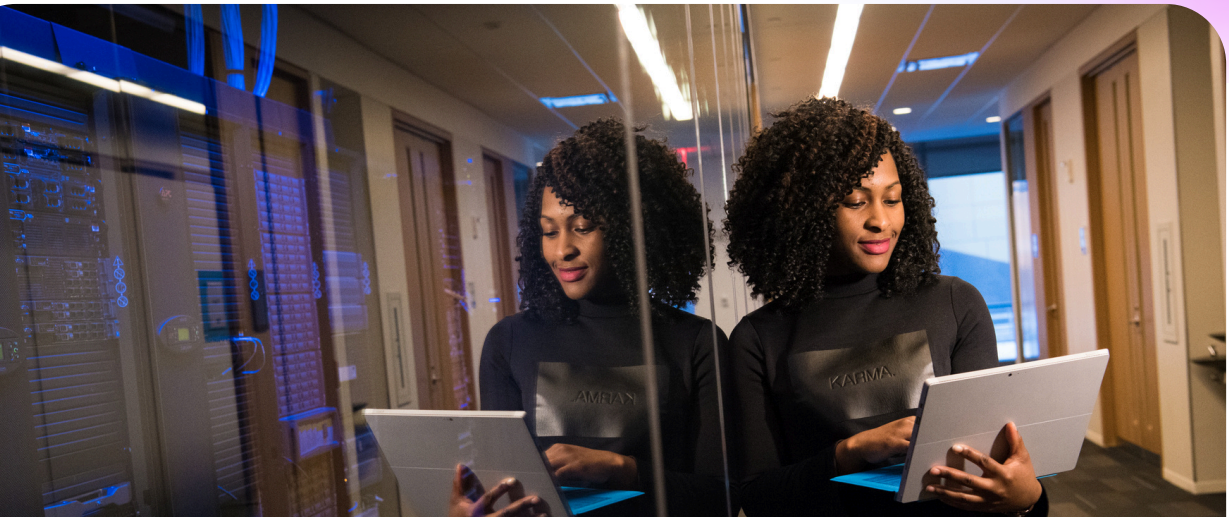
This clause is all about the execution of the plans and processes that are the subject of previous clauses. It deals with the execution of the actions determined and the achievement of the information security objectives, requiring organisations to establish criteria for the required processes and implement those processes accordingly. In recognition of the increased use of outsourced functions in today's business world, these processes also need to be identified and controlled. Any changes, whether planned or unintended need to be considered here and the consequences of these on the ISMS. It also deals with the performance of information security risk assessments at planned intervals, and the need for documented information to be retained to record the results of these. Finally, there is a section that deals with the implementation of the risk treatment plan, and again, the need for the results of these to be retained in documented information.

Clause 9: Performance Evaluation

This clause is all about monitoring, measuring, analysing, and evaluating your ISMS to ensure that it is effective and remains so. This clause helps organisations to continually assess how they are performing in relation to the objectives of the standard to continually improve. You will need to consider what information you need to evaluate the information security effectiveness, the methods employed and when it should be analysed and reported. Internal audits will need to be conducted as well as management reviews. Both must be performed at planned intervals and the findings will need to be retained as documented information. It should be noted that management reviews are also an opportunity to identify areas for improvement.

Clause 10: Improvement

This part of the standard is concerned with corrective action requirements. You will need to show how you react to nonconformities, act, correct them and deal with the consequences. You will also need to show whether any similar nonconformities exist or could potentially occur and show how you will eliminate the causes of them, so they do not occur elsewhere. There is also a requirement to show continual improvement of the ISMS, including demonstrating the suitability and adequacy of it and how effective it is. However how you do this is up to you. ISO/IEC 27001 also includes Annex A which outlines 93 controls to help protect information in a variety of areas across the organization. ISO/IEC 27002 also provides best practice guidance and acts as a valuable reference for choosing, as well as excluding, which controls are best suited for your organisation.



CFS

KEY BENEFITS

76%

Reduces business mistakes

80%

Inspire trust in your business

76%

Helps protect your business

53%

Increase your competitive edge

55%

Helps comply with regulations

CFS

Value Of Certification

In addition to protecting your data and complying with data handling laws like the GDPR, there is a distinct market value to ISO 27001 certification. It is financially prudent to protect your organisation's data and to meet the legal requirements of nations in which you seek to do business. Achieving certification is a valuable and visible proof of your organisation's willingness to meet internationally accepted data security standards. Achieving this international standard is not simply marketing: as well as complying with the GDPR and other related laws such as those aligned with the Directive on Security of Network and Information Systems (NIS Directive), the ability to prove that your organisation complies with ISO 27001 is likely to open business opportunities across the globe. It should be noted that many markets have already shown a desire for ISO 27001 certification, with over 33,000 organisations worldwide having received certification.

CFS

International Recognition

In the United Kingdom, accreditation of certifying bodies is managed by the United Kingdom Accreditation Service (UKAS), which maintains a list of all organisations qualified to certify ISO 27001. Through several agreements with other international bodies, a certification in the UK is recognised across the globe. The European Cooperation for Accreditation (EA) is comprised of 35 national accreditation bodies across Europe (including several associate members further afield). The EA multilateral agreement affirms:

- The equivalence of the operation of the accreditation systems administered by EA members.
- That the certificates and reports issued by organisations accredited by EA members are equally dependable.

This means that certification approved by one member of the EA is accepted across all other member states. ISO 27001 is not only recognised throughout the EU, but also has a broader appeal in other key markets via the International Accreditation Forum (IAF). The IAF ensures that ISO 27001 certification is recognised across the world through a 'mutual recognition arrangement' , agreed by more than 70 national accreditation bodies

CFS

Cyber
Framework
Solutions

Thank You

"The way we work together determines the way we succeed. "

+44 161 4778904
+44 7939 184541

info@cyberframeworksolutions.com