ISO/IEC 27001 Information Security Management

Information security is a common concern for modern organisations, with the increasing volume, accuracy and value of data used in everyday business operations.

Information Security Management Systems (ISMS) involve processes, documents, technologies, and people that help manage, monitor, audit and improve your organisation's information security.

Having an ISMS implemented and reviewed can bring many benefits to an organisation, including, but not limited to:

- Securing all forms of information
- Increasing attack resilience
- Response to evolving and emerging security threats
- Enablement of holistic security-aware culture
- Reducing information security costs by adding layers of redundant defensive technologies

A key component to ensuring that any implemented ISMS is adequate and aligns with security best practices and business goals, the ISO/IEC 27001 international standard sets out a specification to which an effective ISMS must adhere to.

Robust Governance

In the last few years, governance requirements have become increasingly fine-grained, with information technologies now supporting almost every aspect of our organisations.

The role of information security in governance is now better, more clearly defined and increasingly recognised as an area of attention for boards and corporations.

In addition to the need for protecting your data and complying with legislation such as GDPR and the NIS Directive, ISO 27001 certification can bring value to your organisation where meeting the legal requirements of nations in which you seek business, and the protection of data is now financially prudent.

ISMS Development

Managing to prepare for the development of an ISMS can be tricky and involves everyone from management to maintenance staff. ISO 27001 provides a structured approach to developing your ISMS, which includes the following:

Scope Definition

The boundaries and applicability of your ISMS are defined, identifying all the assets, processes, locations, people, and technologies covered in scope by the ISMS.

Developing a Management Framework

Roles and responsibilities for key individuals, such as the Information Security Officer, are clearly defined and allocated.

Senior management is responsible for providing leadership and support for the ISMS. This includes approving the ISMS policy, providing necessary resources, and demonstrating a commitment to information security.

Risk Assessment & Treatment

Risks are identified and evaluated in line with security principles (CIA triad), using standard risk assessment methodology to determine the impact and likelihood of risks. A plan is also created to address risks identified through the risk assessment, outlining how they are handled (mitigated, accepted, or transferred), including implementing necessary security controls.

The business continuity plan outlines the organisation's approach to maintaining business continuity during a disruptive incident. It includes criteria for identifying critical business functions and resources, and guidelines for developing and testing business continuity plans.

Implementing Security Controls

Implementing security controls identified during risk assessment and treatment will be adopted and executed, encompassing technical solutions, policies, procedures, and awareness initiatives that comply with ISO 27001 requirements.

Documentation of ISMS

Comprehensive documentation about the ISMS is made available, including definitions of ISMS processes, policies, and procedures, with such documentation accessible to relevant personnel.

Training & Awareness

Ensure all employees are aware of their defined and allocated roles and responsibilities in maintaining strong information security, with regular training programs to enhance awareness and understanding. All employees are responsible for following the security policies and procedures established by the ISMS.

Monitoring

Implement a system to monitor and measure ISMS performance, such as security controls, incident response and other efficacy metrics.

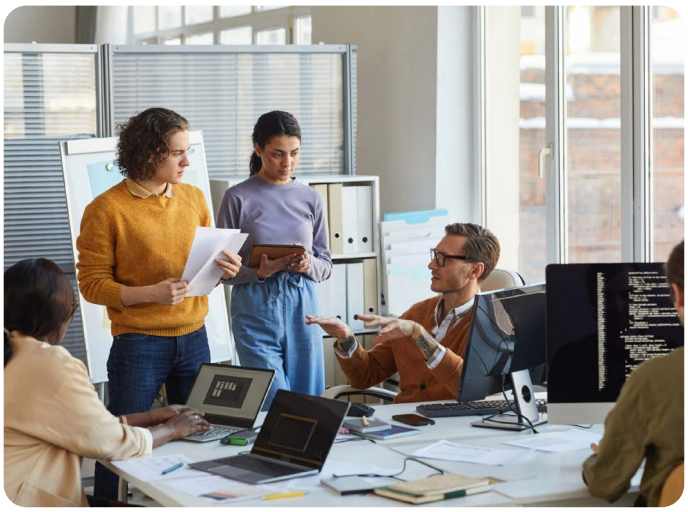
Auditing & Review

Regular internal audits should be conducted to assess ISMS conformity and effectiveness, compliance with ISO 27001 (2013 or 2022 standard) and identify areas for improvement. Regular reviews with management should assess audit findings and review security control performance, addressing non-conformities and implementing corrective measures to mitigate any issues identified.

Certification to ISO/IEC 27001

The process for implementing an ISMS using the ISO 27001 standard can certainly prove your organisation is committed to maintaining strong information security.

If desirable, you can further this commitment and compliance with the ISO 27001 standard by achieving ISO 27001 certification. Typically, a certification body is engaged to conduct the certification assessment, where an approved individual will carry out an external audit of your ISMS in the scope of ISO 27001.



How can Sapphire help?

Sapphire can help you with many aspects of ISO27001, ranging from scoping activities and providing executive oversight to assisting in the development of your ISMS to the new ISO27001 (2022) standard and helping you with certification.

Scoping

Sapphire can carry out an ISO27001 gap analysis to provide you with a current situation (statement of applicability) over the 93 controls which apply.

We can assist with an executive delivery commitment to the various clauses of the standard and develop a Security Improvement Plan.

ISMS Policy Development

Sapphire can advise or assist with various ISMS policies, from review to development. These policies include, but are not limited to:

- ISMS Policy
- Information Security Policy
- BYOD Policy
- Patch Management Policy
- IoT Policy

We can also help you with defining roles and responsibilities, defining an Information Security Manual and other guides for those in your company.

Sapphire can assist and provide procedures relating to suppliers' due diligence, which ensures they meet the same information security requirements.

Furthermore, Sapphire can also help provide guidance for legal, compliance and governance.

Risk Management

Sapphire can help you manage your risks under the standard in many aspects. We can perform risk assessments, develop risk treatment plans, and assist you with building your risk register and policies aligned to the assets you wish to have in scope.

Sapphire can also assist with business continuity, including creating plans, formulating policies, executing disaster recovery plans, and performing tabletop exercises to test your plans.

We can provide training and awareness programs to ensure employees understand their roles and responsibilities in maintaining information security.

On top of this, we can also assist with incident and change management processes to provide a holistic approach, ensuring your risk management aligns with the ISO27001 standard.

Security Controls

Sapphire can provide a wide range of technologies that can assist you with implementing different security controls as part of the ISMS. These include:

- Firewalls
- Vulnerability Management
- Penetration Testing
- Extended Detection and Response
- SIEM
- Incident Response (24x7x365)
- Premium Threat Intelligence Service

Subject Matter Expertise

Sapphire has a 100% ISO27001 pass rate, enabling you to achieve certification on the first attempt and avoid financial and operational costs related to failures. We can streamline your compliance by swiftly identifying vulnerabilities and gaps and offering tailored solutions that align with the ISO27001 standard.

Our teams consist of exceptionally skilled, dependable, ethically grounded consultants and technical experts. Their capabilities and expertise undergo continuous evaluation and improvement to ensure our services are built around the guidance, planning, and protection you need to reach your compliance goals.