SECURANCE

Step-by-step Guide

ISO 27001 Certification.

Content

Getting to Know the ISO 27001 Norm

In this whitepaper, we will provide you with the necessary information on the ISO 27001 standard. The whitepaper consists of information regarding the ISO 27001 norm, the project phases of the ISO 27001 certification, and the benefits of the ISO 27001 standard for your organisation.

As a professional Risk Management Governance, and Compliance firm, we are pleased to provide support with the ISO 27001 certification project within your organisation. We are more than pleased to answer questions you might have regarding the ISO 27001 norm.

ISO 27001

Information Security

ISO 27001 is an internationally recognised standard for information security management systems (ISMS). It specifies the requirements for establishing, implementing, maintaining, and continually improving an ISMS. The standard provides a framework for managing information security risks, encompassing people, processes, and technology.

ISO 27001 certification demonstrates an organisation's commitment to information security and its ability to protect sensitive data. This certification is achieved through an independent audit process conducted by an accredited certification body. The audit assesses the organisation's ISMS against the requirements of the ISO 27001 standard.

The scope of the ISO 27001 certification audit covers the organisation's ISMS, including the policies, procedures, and controls implemented to manage information security risks. It also includes the context of the organisation, its interested parties, and the scope of its ISMS.

ISO 27001 does not prescribe specific controls but rather provides a framework for organisations to identify and implement the controls necessary to address their specific risks. The standard emphasises a risk-based approach, requiring organisations to identify, analyse, and evaluate their information security risks and select appropriate controls to mitigate those risks. A successful audit results in the issuance of an ISO 27001 certificate, which is valid for a defined period, typically three years, subject to periodic surveillance audits.

Information Security Management

Information security management is the process of protecting an organisation's information assets from unauthorised access, use, disclosure, disruption, modification, or destruction. It involves a systematic approach to identifying, assessing, and managing information security risks.
The objective is to ensure confidentiality, integrity and availability of information.

To achieve ISO 27001 certification, service organisations must define their ISMS scope, including the relevant processes, a risk assessment methodology, and a Statement of Applicability (Statement of Applicability) detailing the controls implemented. This documentation should describe the controls and how they address identified risks.

Following certification, service organisations must maintain their ISMS. This means all documented procedures and controls must be actively enforced. Consistent application of these procedures, diligent management of information security processes, and a culture of security awareness within the organisation are crucial for ongoing compliance with the ISO 27001 standard and the continued validity of the certification. This ongoing compliance is typically verified through regular surveillance audits by the certifying body.

Industries

Organisations providing services to other organisations, e.g., Asset/Property Managers, Pension Services Providers, Software as a Service (SaaS)-providers, Infrastructure as a Service (IaaS)-providers, Platform as a Service (PaaS)-providers, and Datacentre Services providers are generally required to certify to the ISO2001 standard.

Phase 1. Scope Definition

How to Define the Scope of your ISO 27001 certification

Defining the scope of your ISO 27001 certification is a critical first step in establishing your Information Security Management System (ISMS). It sets the boundaries for what is included in your ISMS and, therefore, what will be audited for certification.

Prepare the Scope

The preparation of the ISO 27001 scope is a fundamental initial undertaking, establishing the perimeters of the Information Security Management System (ISMS) and defining the areas subject to audit.

This process commences with a thorough comprehension of the ISO 27001 standard. The organisation's information assets, encompassing data classifications, business processes, supporting IT systems, and their respective locations, must be identified.

A precise definition of the ISMS boundary is then required, explicitly specifying inclusions and clearly articulating any exclusions. This definition is formalised in a concise scope statement, supplemented by supporting documentation such as organisational charts, network diagrams, and process maps.

A thorough risk assessment, alignment with organisational business objectives, and consideration of available resources should guide the scope definition. The scope remains a dynamic document subject to regular review and updates, incorporating stakeholder feedback to reflect evolving organisational circumstances. Active engagement of key stakeholders, precise and unambiguous documentation, a pragmatic and attainable scope, and formal approval by top management are essential for successful scope preparation, thereby establishing a robust foundation for the ISMS.
A statement of Applicability is drafted, which acts as a bridge between the information security risks your organisation faces and the controls you implement to mitigate those risks. The Statement of Applicability lists all the information security controls outlined in Annex A of the ISO 27001 standard. These controls are a comprehensive set of best practices for managing information security. For each control, the Statement of Applicability states whether it applies to your organisation. This is where you determine if the control is necessary and relevant to your specific risks and business context.

Competitive Advantage

How an ISO 27001 Certification Gives You an Edge Over Your Competitors

ISO 27001 certification gives a market advantage by building greater trust and confidence in customers and stakeholders, demonstrating compliance with strict information
security controls. Certification distinguishes an organisation from others, especially in data-sensitive industries, and makes it the qualification of choice or a requirement for large business and government contracts. Beyond market positioning, ISO 27001 reduces risk and improves resilience by having proactive risk management and incident response planning, which facilitates business continuity.

Phase 2. Implementation

Step-by-step Approach

1. Planning

In Phase 1, the impact (GAP analysis) of the implementation is determined. Based on the impact and the defined scope of the implementation, a detailed plan is prepared in which the various milestones are identified, and arrangements with management are made.

2. Design

In Phase 2, interviews are held to identify risks, determine the impact and the existing working method, and take note of the information present within the organisation. Documented policies and detailed policies are developed which are aligned with the ISO 27001 standard and your company's business goals.

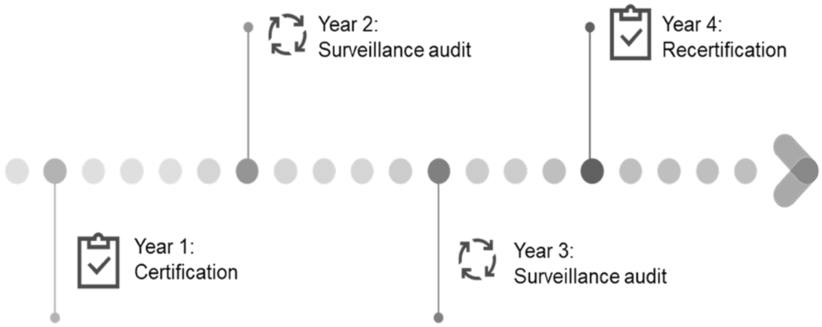
3. Monitoring, review, and improvement

ISO 27001 is a continuous improvement process. Regularly review and update your ISMS to ensure that it remains effective.

Phase 3. The Audit

ISO certification audits

The ISO 27001 certification operated on a three-year cycle.



Year 1: Initial certification audit

The Year 1 Initial Certification Audit for ISO 27001 represents a significant milestone in achieving certification. It is a comprehensive assessment of your Information Security Management System (ISMS) to ensure it meets the ISO 27001 standard. In this stage, the ISMS will be audited for design and implementation. The auditor assesses whether all the controls of the ISO 27001 in scope are achieved.

Year 2: Surveillance audit

During the first surveillance audit, the auditor will concentrate on specific areas of your ISMS, often those identified as higher risk or areas where changes have been made since the initial certification. They might also check up on the status of any corrective actions from the initial audit. Successful completion of the surveillance audit is essential for maintaining your ISO 27001 certification.

Year 3: Surveillance audit

The second surveillance audit buils on the first surveillance audit, to verify whether you are continuously maintaining and improving your ISMS while effectively meeting the ISO 27001 standards requirements.

Year 4: Re-certification audit

The ISO 27001 certification audit is a comprehensive assessment of your Information Security Management System (ISMS) to ensure it meets the ISO 27001 standard. In this stage, the ISMS will be audited for design and implementation. The auditor assesses whether all the controls of the ISO 27001 in scope are achieved.

Key Benefits

Of ISO 27001 certification

Experience the Benefits of ISO 27001 Certification

ISO 27001 certification are used by organisations as a marketing tool. New and existing customers immediately recognise that they are dealing with a reliable party. Organisations that do not have such reporting may be missing out on important new opportunities. During the sales process, it is common for a customer to ask their supplier to fill in a questionnaire to gain insights into the current maturity level of the organisation.

Providing you with an ISO 27001 certificate is likely to provide effective answers to these questions. It will speed up the process considerably. This will also provide the customer with the feeling and confidence that processes are indeed in order.

Introducing Securance

Invest in Efficiency, Value, and Partnership

- **Analyse Risks**
- **Plan the Project**
- **Prepare System Descriptions**
- **Perform a Readiness Assessment**

Implementing ISO 27001 requires effective planning, leadership involvement, thorough analysis of processes and reliable resources and project management.

Securance originates from a 'Big Four' audit firm and was founded in 2004. The result of our background is that we work in accordance with the highest professional standards and have experience in working with tight deadlines. We live by our professional standards, and we always deliver the highest quality whilst continuously striving to meet our clients' needs.

As a consequence of our flat structure and efficient communication framework, we can respond quickly to your requirements. Choosing Securance implies selecting a professional organisation but also choosing a personal approach. Effective project management, our experience with implementing risk management frameworks in your industry, and professionalism are, in our opinion, the foundation for excellent results.

As Securance, we believe that a good understanding, clear communication, and knowledge of our clients' industry are essential for delivering added value to you as our client. Based on this approach, we will inform you of the relevant changes in laws, regulations, and other important developments.

SECURANCE
BE SURE

Our Satisfied Customers

References

FUJITSU

colt

Planday

NTT

Templafy

SIG Software Improvement Group

CUSHMAN & WAKEFIELD

axians

Aareon WE MANAGE IT FOR YOU

eurofiber

channel mechanics

Canon

SECURANCE
BE SURE

Securance Ltd.

63-66 Hatton Garden
London EC1N 8LE, UK
+44 20 351 446 56
www.securance.co.uk

Securance BV

Reactorweg 47
3542 AD Utrecht
+31 (0)30 2800888
www.securance.nl