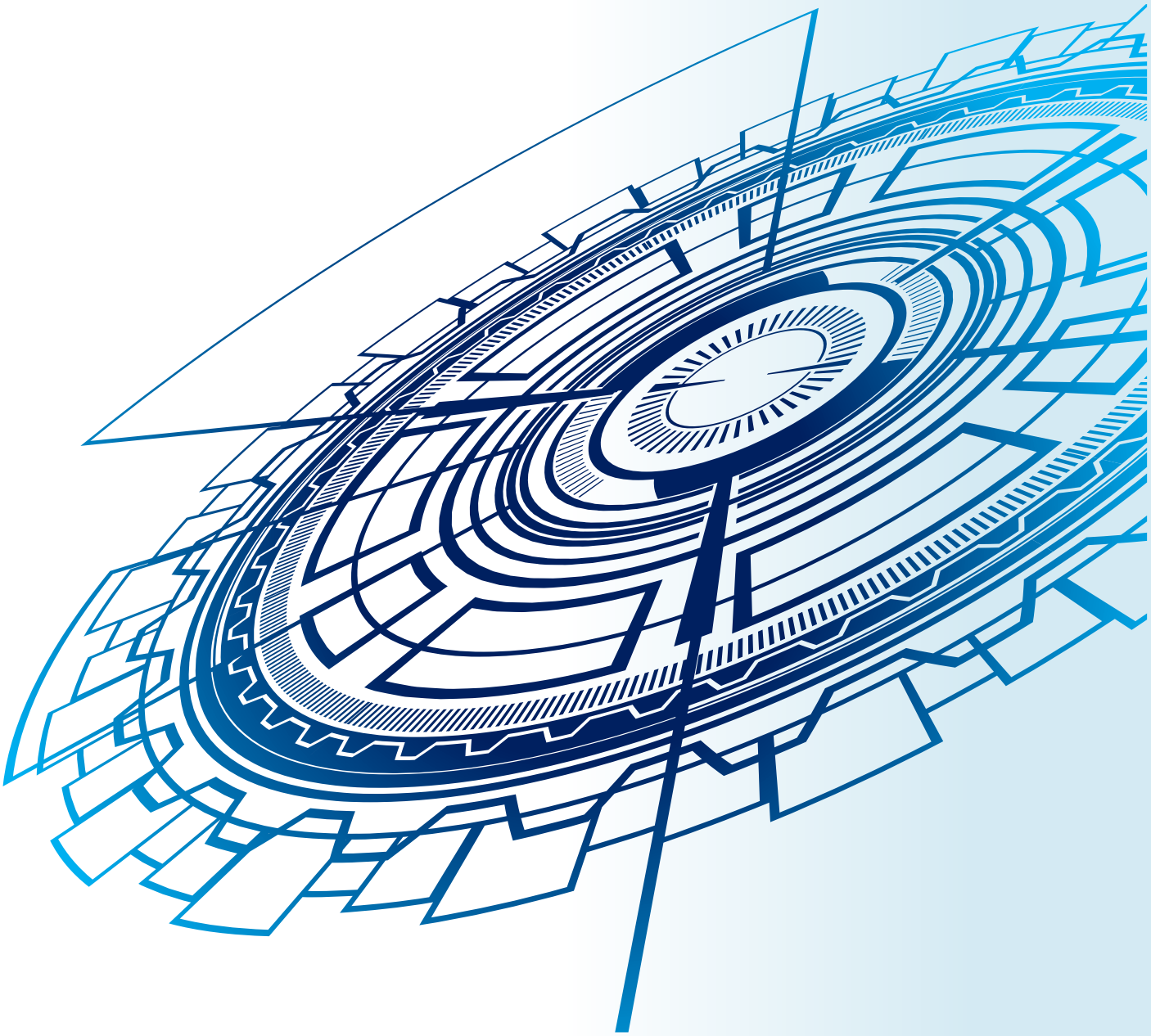
ISO 27001:2013

IMPLEMENTATION GUIDE



WHY IS ISO IMPORTANT?

The International Organisation for Standardisation (ISO) is a multi-national organisation that puts forth internationally recognised standards that provide structured frameworks of doing business efficiently and effectively. ISO is an independent, non-governmental organisation, consisting of 164 member countries. ISO was initiated with the idea of answering a fundamental question: "What is the best way to do business?"

The ISO certification mark confirms that your business complies with certified international practices to ensure that your organisation is a reliable and trustworthy service provider, attracting prospective clients and stakeholders.

Customers, regulators, and governments rely on ISO standards to help develop better regulations for businesses in their country. By trusting globally recognised experts to deliver globally agreed upon standards and template frameworks, you can be assured that ISO standards are worth complying to.

ISO Certifications are a means to qualify businesses. This ensures that a certified organisation has a robust Business Management System comprising of Policies, Objectives, Plans, Processes, Procedures, Risk Assessments, Consistent Forms, Templates, and Standardisation. The purpose of standardisation is to streamline production in various industries, ensuring the quality, consistency, and safety of products and services, while supporting global collaboration and compatibility.

There are many benefits of standardisation for businesses. Customer satisfaction is a key element to success for any business. By complying with various ISO standards, you will ensure that your products and services are delivered at optimal levels of quality. ISO certification is seen as a stamp of approval. By implementing these standards, it increases and streamline productivity, cut costs, and reduce errors.

ISO implementation will aid both short- and long-term business strategies to help a business run smoothly, no matter the size or industry of the business. ISO Management Systems gives every business a competitive advantage over a competitor that does not comply with or implement such a framework in their business. By implementing a Management System that complies with international standards, you will ensure customer satisfaction through quality products and services.

INTRODUCTION

International Standards are long used as a business improvement tool to help drive continual improvement and deliver results in your organization. It is well known that implementation of a Management System transcends well past a piece of paper, and enters the real world as not only being a “stamp of approval” but also an operational tool which results in competitive advantage and an instrument which leverages growth.

Working in hand with the culture of your organisation, Management Systems present a fool-proof strategy to ensure that customer satisfaction, quality, and performance form a solid foundation to your organisation. As technological advantages disrupt industries, and leave many poorly-prepared companies in their wake, the framework provided by these international Standards help predict volatility, and allow you to get ahead of the curve by predicting changing requirements, ensuring your satisfaction levels shift with the tides of change. International Standards are rigid enough to ensure consistent and comparable results, but flexible enough to bend and sway with the requirements of your organisation.

This Implementation Guide will assist you through the process of establishing an Information Security Management System (ISMS) in accordance with the requirements of ISO/IEC 27001:2013.

NOTE: Specific reference should be made to the ISO/IEC 27001:2013 STANDARD: UNVEILED section of this document.

This guide is laid out to cover the specific requirements of each clause of the Standard, to give additional detail and provide direction. Specific tips have been included, in addition to clause descriptions, to ensure that your establishment and implementation process runs as smoothly as possible. It is also important to note that many Management Systems are closely related and may share the same requirements. Although the clause structure may appear identical, there are multiple technical, legal, and other requirements that must be met to be certified.

Furthermore, as this guide does not contain the text of the ISO/IEC 27001:2013 Standard, users are recommended to obtain a copy from their national standards body or from ISO, either directly via sales@iso.org or via the Internet from www.iso.org.

> Quality is never an accident; it is always the result of high intention, sincere effort, intelligent direction, and skilful execution; it represents the wise choice of many alternatives.
>
> - *William A. Foster*

COMMITMENT

FEEDBACK

MOTIVATION

REVIEW

KNOWLEDGE

ISO/IEC 27001:2013 STANDARD: UNVEILED

Implementation Guide

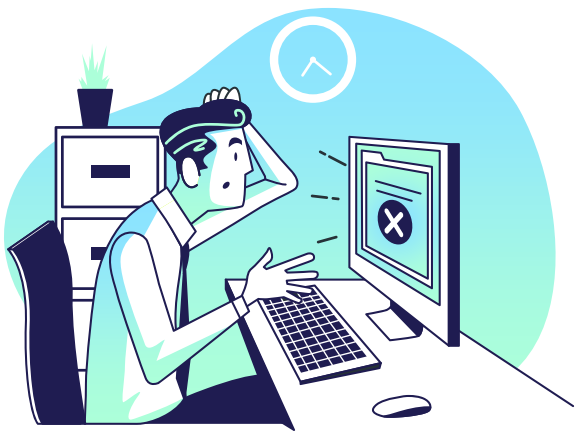
These state-of the-art templates enable your company to utilize robust and effective processes to protect the confidentiality, integrity, and availability of information. Based on promoting a risk and security awareness culture, as well as assessment of risks and the treatment thereof, these templates utilize multiple avenues to ensure focused results. The multiple benefits of utilizing templates for ISO/IEC 27001:2013 include significantly improved control, compliance with legal, statutory, and regulatory requirements, secure information exchange, exposure reduction, and protection of company assets. As the security of company information and assets becomes an increasing global concern, conformance to the ISO/IEC 27001:2013 Standard has become a must. With concentration on best practice principles, systematic risk treatment, and continual improvement, these templates will allow your company to meet and exceed expectations whilst promoting stakeholder confidence. Alleviating your administrative burden and frustration regarding often difficult to interpret clauses and expectations – these templates offer a unique advantage by being adaptable to your company's size and industry. These templates allow you to take full advantage of the framework to provide consistent and reliable results – with a competitive edge.

Purpose of Toolkit

Building a Management System from the ground is a daunting and daring task – yet it is the cornerstone of every successful certification process. We have assisted various organizations to achieve certification to a range of Standards – showcasing our expert ability to provide direction and support. Our WWISE ISO Experts have spent many years perfecting, streamlining, and updating our templates to ensure your company can implement ISO/IEC 27001:2013 in-house, with practiced guidance and support.

These templates are formulated to integrate seamlessly with any existing Management Systems – and present a simple, effective, and fully-covered approach to compliance. These templates contain effective tools to simplify the implementation process and demonstrate the effective operation of your Information Security Management System.

Designed to save time and effort in the preparation and processing of the Standard by providing fully-fledged documentation – simply providing the assistance of a Consultant, without their presence!



Additional Information

Text:

- Green text are examples only.
- Red text are guidelines which require to be replaced with the correct information.

Document Type and Numbering:

- Document Type is to be determined by the following conventions:
  - POL – Policies
  - PF – Process Flows
  - PRO – Procedures
  - FT – Forms and Templates
  - WI – Work Instructions
- Document numbering is to be in sequential order, with the following convention:
  - (Document Type-Sequential Number) e.g. The first Policy will be labelled POL-001.

Corporate Identity (CI) Manual:

- Your company should have a document in place mandating the following:
  - Naming (exclusive company name)
  - Logo
  - Color palette (color)
  - Corporate font
  - Business card
  - Letterhead
  - Envelop

Logo:

- The Logo is to be placed in the header box (top right-hand corner) of the Word page.
- This image is to be taken as it stands in the Corporate Identity (CI) Manual.

Clause 1: Scope

This section outlines the scope of the Information Security Management System (ISMS). This must be consistent with your information security policy. The intended outcomes should enhance information security performance and fulfil compliance obligations.

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

This section explains any relevant terms and definitions. Please refer to the terms and definitions contained in ISO/IEC 27000.

Clause 4: Context of the organization

This section is responsible for detailing the general requirements mandated for an ISMS. Within this, an understanding of your organisational context is required. As expected, the information security issues that may affect your organisation are largely dependent on size and industry. The needs and expectations of interested parties who could influence business decisions must also be considered. Through consideration of the context of the organisation, which covers the internal, external, and information security context (your information or information that is entrusted to you by 3rd parties), all direct and indirect consequences because of information interaction are to be determined.

Implementation documentation:

- List of Legal Regulatory Contractual and other Requirements
- List of Internal and External Issues
- Strategic Plan
- Information Security Scope
- List of Interested Parties
- Overall Process Sequence and Interaction

Clause 5: Leadership

This section is responsible for determining the involvement of top management in the ISMS. Top management is required, by the standard, to demonstrate leadership and commitment to the ISMS. This leadership and support are best shown through the roles, responsibilities, and authorities top management must define. An Information Security is also required to be signed off by top management to demonstrate commitment to business practices that will not cause harm to information security status, as well as legal and other requirements as stipulated.

Implementation documentation:

- Specification of Information System Requirements
- Incident Log

- Information Security Policy
- Identification of Requirements Procedure
- Incident Management Procedure
- Security Clauses for Suppliers and Partners
- ISMS Letter of Appointment
- Meeting Minutes Template

Clause 6: Planning

This section of the Standard emphasises the importance of having resources in place to ensure the intended outcome(s) of the ISMS are achieved – this is attained through risk identification and analysis. In addition to this, the role of risks and opportunities, as well as how these risks and opportunities will be identified and planned around regarding the ISMS. Legal requirements are also to be determined to ensure your company addresses specific actions. The setting of objectives and planning to achieve them must also be defined. In addition to this, it should be noted that ISO/IEC 27001:2013 is based on the "Plan-Do-Check-Act" (PDCA) cycle. Organizations are also required to produce a "Statement of Applicability" (SoA).

Implementation documentation:

- Risk Assessment and Risk Treatment Methodology
- Statement of Applicability
- List of Objectives

Clause 7: Support

This section relates specifically to the resources used and needed by the ISMS, as well as communication and documentation. As for human resources, adequate assessment of competence, training, and ISMS awareness must be demonstrated. The control of documentation relevant to the ISMS is also determined. Internal and external communication relevant to the ISMS is also to be determined. This section of the Standard also stipulates that communication regarding the Information Security Policy and how employees contribute to the ISMS must be shown. There is also an emphasis on controlling access to documented information, which reflects the importance of information security.

Implementation documentation:

- Documents Change Request Sheet (Master Index)
- Inventory of Assets
- Training and Awareness Plans
- Control of Documents and Records Procedure
- Communications Procedure

Clause 8: Operation

This section determines how the control of operations will be planned for. For operations with a significant information security impact, written processes should be established. It should be specifically noted that these processes must incorporate the solutions identified in clause 6.

Emergency information security situations must also have plans and response measures in place. While referencing the increased use of outsourced functions, these processes also need to be identified and controlled. Any changes, whether planned or unintended, also need to be considered here and the consequences of these on the ISMS.

Implementation documentation:

- Operating Procedures for Information and Communication Technology
- Risk Assessment
- Risk Assessment and Treatment Report

Clause 9: Performance evaluation

This section determines how ISMS processes (and legal requirements) will be monitored, measured, analysed, and evaluated to ensure compliance. With internal audits, problems and corrective measures will be determined. Furthermore, management must review the ISMS to ensure its continuing suitability and adequacy. Management must also determine that the ISMS is being used effectively. Internal Audits will need to be carried out as well as Management Review Meetings.

Implementation documentation:

- Internal Audit Plan
- Internal Audit Programme or Schedule
- Internal Audit Report
- Management Review Meeting Agenda
- Management Review Meeting Minutes
- Opening Closing Meeting Register
- Internal Audit Procedure
- Management Review Procedure
- Monitoring Measurement Analysis and Evaluation Procedure

Clause 10: Improvement

As for most ISO Standards a commitment to continual improvement is important. This section relates specifically to non-conformities that are to be addressed, along with their corresponding corrective and continual improvement actions. Improvement relies heavily on identifying potential issues and using these opportunities to progress processes and reduce information security impacts. ISO/IEC 27001 also includes Annex A which outlines 114 controls to help protect information in a variety of areas across your organisation. It should also be noted that ISO/IEC 27002:2013 also provides best practice guidance and acts as a valuable reference for choosing as well as excluding which controls are best suited for your organization.

Implementation documentation:

- NCR & CAR Index
- NCR & CAR Report
- Non-conformance and Corrective Action Procedure

ISO/IEC 27001 Controls List: the 14 control sets of Annex A

Annex A.5 – Information security policies (2 controls)

This annex ensures policies are written and reviewed in line with the overall direction of the organisation's information security practices.

Annex A.6 – Organisation of information security (7 controls)

This annex covers the assignment of responsibilities for specific tasks and is divided into two sections.

- Annex A.6.1 – ensures the organisation has established a framework that can adequately implement and maintain information security practices within the organisation.
- Annex A.6.2 – addresses mobile devices and remote working. It's designed to make sure that anyone who works outside of the office – either part-time or full-time – follows appropriate practices.

Annex A.7 – Human resource security (6 controls)

This annex covers employees and contractors' responsibilities, to ensure these parties understand their responsibilities.

- Annex A.7.1 – addresses individuals' responsibilities prior to employment.
- Annex A.7.2 – covers their individuals' responsibilities during employment.
- Annex A.7.3 – addresses individuals' responsibilities when they no longer hold that role – either because they've left the organisation or changed positions.

Annex A.8 – Asset management (10 controls)

This annex contains 3 sections, and concerns the way information assets are identified, and defines appropriate protection responsibilities.

- Annex A.8.1 – involves the organisations identifying information assets within the scope of their ISMS.
- Annex A.8.2 – information classification. This process ensures that information assets are subject to an appropriate level of defence.
- Annex A.8.3 – is about media handling, ensuring that sensitive data isn't subject to unauthorised disclosure, modification, removal, or destruction.

Annex A.9 – Access control (14 controls)

This annex is in place is to ensure that employees can only view information that's relevant to their job. It's divided into four sections, addressing the business requirements of access controls, user access management, user responsibilities and system and application access controls, respectively.

Annex A.10 – Cryptography (2 controls)

This annex is about the management of sensitive information, as well as data encryption. Its two controls are designed to ensure that organisations use cryptography properly and effectively to protect the confidentiality, integrity, and availability of data.

Annex A.11 – Physical and environmental security (15 controls)

This annex addresses organisation's physical and environment security. It's the largest annex in the Standard, containing 15 controls separated into two sections.

- Annex A.11.1 – to prevent unauthorised physical access, damage or interference to organisation's premises or the sensitive data held therein.
- Annex A.11.2 – deals specifically with equipment. It's designed to prevent the loss, damage, or theft of an organisation's information asset containers – whether that's, for example, hardware, software or physical files.

Annex A.12 – Operations security (14 controls)

This annex ensures that information processing facilities are secure and is comprised of seven sections.

- Annex A.12.1 – addresses operational procedures and responsibilities, ensuring that the correct operations are in place.
- Annex A.12.2 – addresses malware, ensuring that the organisation has the necessary defences in place to mitigate the risk of infection.
- Annex A.12.3 – covers organisations' requirements when it comes to backing up systems to prevent data loss.
- Annex A.12.4 – is about logging and monitoring. It's designed to make sure that organisations have documented evidence when security events occur.
- Annex A.12.5 – addresses organisations' requirements when it comes to protecting the integrity of operational software.
- Annex A.12.6 – covers technical vulnerability management and is designed to ensure that unauthorised parties don't exploit system weaknesses.
- Annex A.12.7 – addresses information systems and audit considerations. It's designed to minimise the disruption that audit activities have on operation systems.

Annex A.13 – Communications security (7 controls)

This annex concerns the way organisations protect information in networks. It's divided into two sections.

- Annex A.13.1 – concerns network security management, ensuring that the confidentiality, integrity and availability of information in those networks remains intact.
- Annex A.13.2 – deals with the security of information in transit, whether it's going to a different part of the organisation, a third party, a customer or another interested party.

Annex A.14 – System acquisition, development and maintenance (13 controls)

The objective of Annex A.14 is to ensure that information security remains a central part of the organisation's processes across the entire lifecycle. Its 13 controls address the security requirements for internal systems as well as those that provide services over public networks.

Annex A.15 – Supplier relationships (5 controls)

This annex concerns the contractual agreements organisations have with third parties. It is divided into two section.

- Annex A.15.1 – addresses the protection of an organisation's valuable assets that are accessible to, or affected by, suppliers.
- Annex A.15.2 – is designed to ensure that both parties maintain the agreed level of information security and service delivery.

Annex A.16 – Information security incident management (7 controls)

This annex is about how to manage and report security incidents. Part of this process involves identifying which employees should take responsibility for certain actions, thus ensuring a consistent and effective approach to the lifecycle of incidents and response.

Annex A.17 – Information security aspects of business continuity management (4 controls)

The aim of Annex A.17 is to create an effective system to manage business disruptions. Its divided into two sections.

- Annex A.17.1 – addresses information security continuity – outlining the measures that can be taken to ensure that information security continuity is embedded in the organisation's ISMS.
- Annex A.17.2 – looks at redundancies, ensuring the availability of information processing facilities.

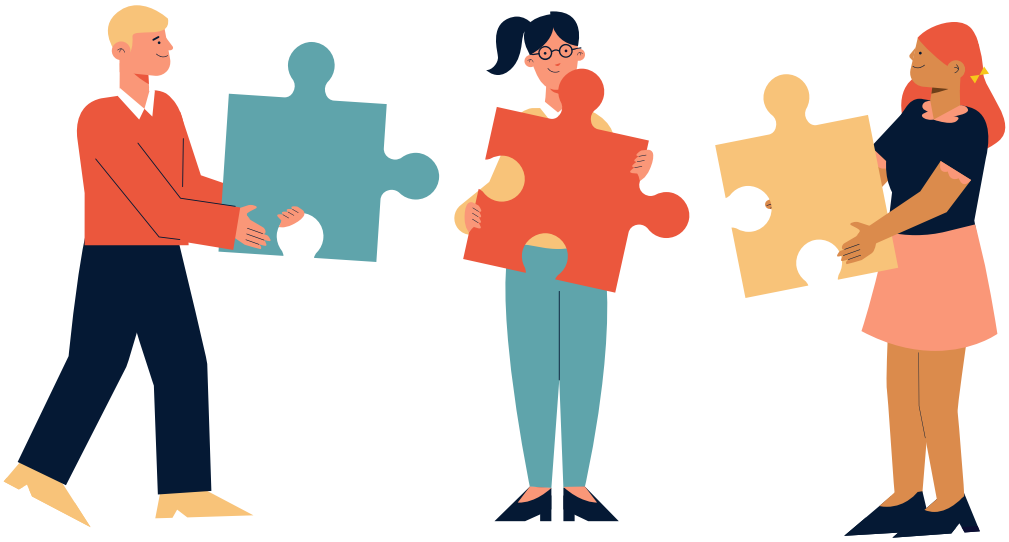
Annex A.18 – Compliance (8 controls)

This annex ensures that organisations identify relevant laws and regulations. This helps them understand their legal and contractual requirements, mitigating the risk of non-compliance and the penalties that come with that.

ISO/IEC 27001 Controls List: Annexure A

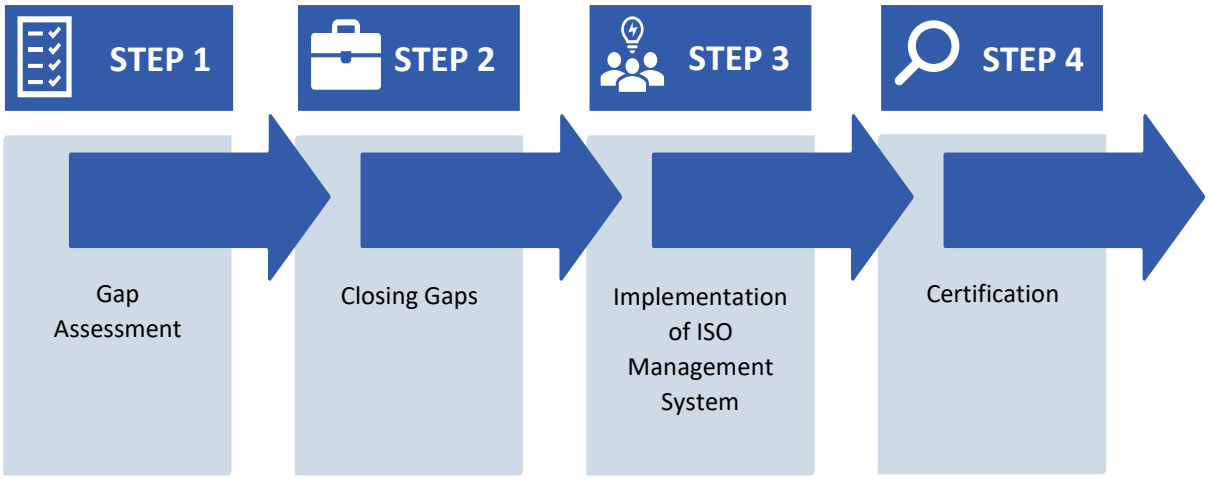
Implementation documentation:

- Acceptable Use of Assets Policy
- Access Control Policy
- Backup Policy
- Bring Your Own Device Policy
- Change Management Policy
- Clear Desk and Clear Screen Policy
- Configuration Management Policy
- Cryptographic Controls Policy
- Disaster Recover and Business Continuity Policy
- Information Classification Policy
- Password Policy
- Removable Media Policy
- Retention Destruction Deletion and Decommissioning Policy
- Secure Development Policy
- Supplier Security Policy
- Teleworking Policy



CERTIFICATION PROCESS

Any organisation wishing to become ISO certified, needs to implement, and maintain an ISO Management System. The Steps that are recommended for an organisation to become ISO certified are as follows:



Step 1 – Gap Assessment

Why do organisations need gap assessments?

- To understand the organisation's current conformance to the ISO Standard of their choice.
- To identify the relevant documentation and records the organisation might already have which are aligned to the standard and identify how to map it to the ISO Standard's requirements.
- To indicate the amount of work required to conform to the ISO standard and to comply to legal requirements.

What are the outputs of the Gap Assessment?

- A Gap Assessment report indicates the current conformance to the standard and the performance of its Management System.
- An obligation free proposal to assist the organisation in closing the identified gaps to conform to the standard with a project plan for implementation and preparation for certification.

Step 2 -Closing Gaps

- Gaps are closed from a documentation and governance perspective according to the standard.
- Awareness Training for all Staff on the importance of ISO, the benefits of ISO certification and the requirements required per role/ individual in the company.
- Information is gathered to understand the respective roles, responsibilities, processes, and procedures.
- Templates for all documentation are standardised and aligned to the corporate identity.
- The Management system is documented and aligned to the standard's requirements.
- Risk management and the specific plans aligned to the standard are focused on and forms are created to collect data to generate Statistics.

Step 3 – Implementation of the ISO Management System

- ISO management system documentation are implemented and records of at least 3 – 6 months are generated.
- On the job training and Workshops on how to use the management system are conducted.
- Internal audit training and maintenance training are conducted to ensure skills transfer.
- Internal audits (dress rehearsals) are conducted with workshops on non-conformances, corrective actions, the updating of risk assessments and the management system if required.
- A management review is conducted. During the management review an action plan is created to ensure all items, either capital or operational expenditure, are managed and documented.

Step 4 – Certification

Key points to consider when choosing a certification body:

- Is the Certification Body accredited? Logos to look out for are: South African National Accreditation System (SANAS), United Kingdom Assurance Services (UKAS), International Accreditation Forum (IAF), Deutsche Akkreditierungsstelle (DAkkS) and many more.
- There are multiple certification bodies globally, it is important that the certification bodies are accredited and being audited by an accreditation body as mentioned above. This ensures credibility of the certification body and respective clients would want to note that the certification was not attained through the internet or purchased, as each certification body is audited by an accreditation body to the ISO 17021 standard.

Who are the different certification bodies?

- British Standards Institute (BSI)
- TUV Nord
- TUV Rhineland
- TUV Sud
- South African Bureau of Standards (SABS)
- Standard Global Service (SGS)
- Bureau Veritas

What is the difference between Single Site and Multi-Site Certification?

- Single Site Certification –One site/location and its departments (HR, Finance etc) and Processes (Recruitment, Induction, Creditors and Debtors) are audited.
- Multi-Site Certification – Organisations with various sites or offices across the country or world require multi-site certification. The sites are sampled over a 3-year period. The Initial Stage 2 audit will be conducted for all sites.

MAKING YOUR MANAGEMENT SYSTEM WORK FOR YOU

- Top management commitment is key to making this a success.
- Engage the whole business with good internal communication.
- Keep staff informed of what's going on, create a team or assign a champion, as this will increase motivation. This could include a well communicated plan of activities and timescales.
- Motivate staff involvement with training and incentives.
- Think about how different departments work together to avoid silos. Make sure the organization works as a team for the benefit of customers and the organization.
- Review systems, policies, procedures, and processes you have in place – you may already do much of what's in the standard, and make it work for your business.
- Speak to your customers and suppliers. They may be able to suggest improvements and give feedback on your service.
- Train your staff to carry out internal audits. This can help with their understanding, but it could also provide valuable feedback on potential problems or opportunities for improvement.
- Get customer and supplier feedback on current quality management.
- Establish an implementation team to get the best results.
- Map out and share roles, responsibilities and timescales.
- Motivate staff involvement with training and incentives.
- Share knowledge and encourage staff to train as internal auditors.
- Regularly review your system to make sure you are continually improving it.

We are what we repeatedly do. Excellence, then, is not an act, but a habit.

- Aristotle