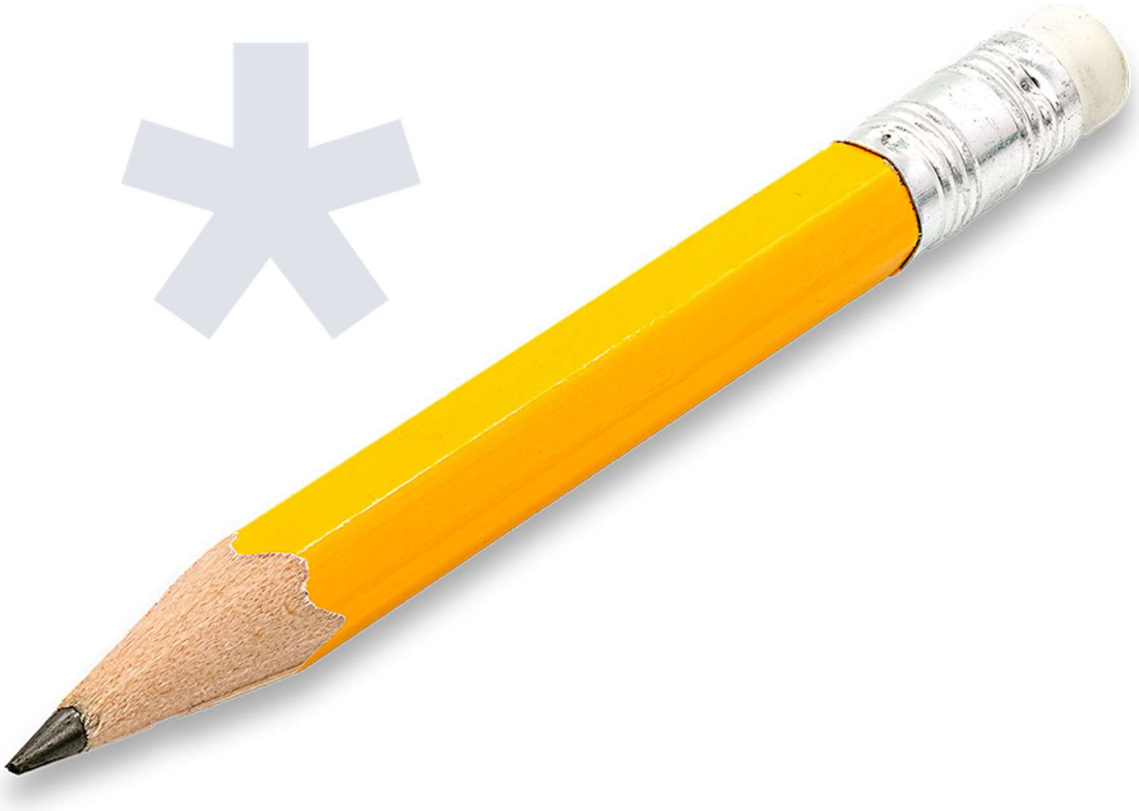

ISO:27001 Readiness Service

Service Description

smartbloc.

norm.™
*Reassuringly dull cyber security

*Reassuringly dull cyber security

CONTENTS

1.0 What is ISO27001? 3
2.0 Implementing an ISO27001 compliant ISMS 3
3.0 Service onboarding and delivery 3
3.1 Stage 1 – Gap analysis 3
3.2 Stage 2 – Implementation 4
3.3 Stage 3 – Mock Audit 5
3.4 Stage 4 – Certification 5
4.0 Service Availability 5

*Reassuringly dull cyber security

1.0 What is ISO27001?

ISO27001 is the international standard for information security. The standard aims to protect the Confidentiality, Integrity, and Availability of information in all forms and types. This information could be financial information on paper, operational data within a spreadsheet, or employee details stored by a supplier. Unlike other standards, ISO27001's risk-based approach allows for a pragmatic implementation of controls designed to protect the organisation's information bearing assets.

Organisations that have implemented an Information Security Management System (ISMS) will have the tools required to handle information security risks on an ongoing basis, methodologies to continually improve their security posture, and a suite of policies and processes dealing with legal, physical, and technical security controls.

2.0 Implementing an ISO27001 compliant ISMS

Typically, when implementing an ISO27001 compliant ISMS, an organisation will need to go through 4 steps:

1. A Gap Analysis to tell you how far the organisation is from compliance.
2. An implementation project.
3. A re-check or mock audit.
4. A certification audit (provided by an approved certification body).

norm's ISO27001 Readiness Service provides access to a fully qualified norm. information security consultant for as much or as little of the implementation process as an organisation requires. This could mean that norm. simply performs a gap analysis to provide the customer with a complete picture of their current position and what needs to be done, or norm. can help guide and manage the organisation through the complete process to certification.

3.0 Service onboarding and delivery

The customer is welcome to determine how involved norm. should be in their ISO27001 readiness programme. As a minimum, this should include a gap analysis. Once an order is received, a member of the norm. Customer Experience team will take ownership of the order and contact you to introduce themselves as the project lead. They will arrange a Welcome call with the customer to introduce the process, outlining who will be responsible for each element of the process.

3.1 Stage 1 – Gap analysis

* The appointed norm. Information Security consultant will provide a list of mandatory documentation, and a mechanism for the consultant to review existing documentation will be agreed. This will usually be via the smartbloc.LIVE portal. norm. will provide your designated administrator with a login to the platform. They can then add additional users as required.

- Your key stakeholders will attend workshops with the norm. consultant to determine whether current working practices comply with ISO27001 and are reflective of your own documentation to the extent that it already exists.
- Norm will produce a report containing recommended actions that will need to be completed prior to undertaking an external ISO27001 certification audit, along with a budgetary level of effort estimate.
- Additionally, Norm will also highlight any other risks that may have been identified during the documentation review or workshops.
- After the Gap Analysis there will be a natural break in the service. The results of the Gap Analysis will inform the effort and time required to complete the implementation of an ISO27001 compliant ISMS.

3.2 Stage 2 – Implementation

The above Stage can be completed as a separate independent engagement without committing to a full Readiness engagement. However, for a successful Readiness engagement to be delivered, a Gap Analysis must first be conducted by a norm. Information Security consultant either as a standalone engagement or part of the Readiness service.

Once the results of the Gap Analysis have been produced and communicated to the customer, norm. can help with the completion of recommended actions as required. In addition, norm. can advise the most effective and efficient methods to build and operate the ISMS and provide access to an online ISMS management platform to help the organisation establish a functioning and relevant ISMS in the shortest possible timeframe.

- norm's involvement in the completion of these actions will be either direct or advisory, depending on the action itself. The level to which the customer requires norm. to be involved in the implementation phase are typically driven by factors such as, customer resource and expertise availability, budget, and the current level of information security maturity that exists within the organisation today.
- Direct involvement may include, but is not limited to:
    - Writing policies.
    - Performing risk assessments.
    - Training key stakeholders in the requirements of ISO27001.
    - Establishing the management review and internal audit planning.
    - Fully managing the implementation and owning the outcome objective i.e., to achieve certification.
- In an advisory capacity norm. may:
    - Advise on the sustainability of technical controls/solutions.
    - Review proposed changes to the ISMS.
    - Provide guidance on the implementation of security controls.
    - Act as an independent and objective oversight to ensure the implementation will pass external audit examination.

3.3 Stage 3 – Mock Audit

This stage will be either a full or partial repeat of the Gap Analysis, however the mock audit will focus on evidence gathering and proving compliance to the standard, whereas the Gap Analysis service is an exploratory activity.

The benefits of performing mock audits are:

* The mock audits will produce reports which can be used as evidence of an internal audit programme.
* They provide confidence ahead of the certification audit.
* They can be used to train the customers own internal audit team.

3.4 Stage 4 – Certification

The customer will undertake a certification audit provided by an accredited certification body. If successful, the ISO27001 certificate will be awarded. norm. can be present in these audits, at the customers discretion, to provide assistance as required and to hold debriefs with interviewees.

4.0 Service Availability

The norm. Information Security consultants and Customer Experience teams are available during UK business hours, Monday to Friday 09:00 to 17:30, excluding public holidays.

The Customer Experience team will be on hand to provide advice and assistance for any queries or issues should this be required.