norm cyber

ISO27001 Readiness Service

Service Description

V1.0 January 2025

Contents

1. Service Description

1.1. 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.

1.2. What is ISO27001 Readiness

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

1. A gap analysis to identify how far the Customer 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.

+44 (0) 203 855 6215 | info@normcyber.com | normcyber.com

2. Service Operation

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 the Order is received, a member of the Norm Customer Experience team will take ownership of the Order and contact the Customer 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 delivery.

2.1. 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 portal. Norm will provide an administrator, designated by the Customer, with a login to the platform. They can then add additional users as required.
- The Customer's key stakeholders will attend workshops with the Norm consultant to determine whether current working practices comply with ISO27001 and are reflective of the Customers 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.

2.2. Stage 2 – Implementation

The gap analysis 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 ISO27001 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 will recommend that the Customer invests in Norm's preferred 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 is typically driven by factors such as, Customer resource, 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

2.3. 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 outcomes that result from conducting mock audits include,

- The production of reports, which can be used as evidence of an internal audit programme
- Providing confidence and experience of being audited ahead of the external certification audit, and
- They can be used to train the customers own internal audit team.

2.4. 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 Customer's discretion, to provide assistance as required and to hold debriefs with interviewees.

+44 (0) 203 855 6215 | info@normcyber.com | normcyber.com

3. Customer Obligations

Once the Order is accepted, the Customer shall,

- provide an Authorised Representative who shall be the Customers Administrator for the Services and responsible for creating and managing access for other Customer End Users who need access to the Service or Smartbloc portal
- agree a timely schedule with Norm's Information Security Consultant to conduct the necessary workshops to enable Norm to deliver the Services
- provide any documentation, policies or process, to the extent that it already exists, within ten (10) Working days after it has been requested by Norm's Information Security Consultant
- ensure that all necessary notices have been provided, and all required consents and/or approvals have been obtained, in order to allow Norm to process the Customer's Data in connection with the Services
- use the Services only in accordance with this Agreement, and all applicable laws and regulations
- where an external certification audit is required, be responsible for scheduling, agreeing and paying the costs of the external certification audit directly with the chosen external certification audit body.

The Customer shall not,

- make the Services available to anyone other than the Authorised Representatives
- sell, resell, rent, lease, lend, loan, distribute, sublicense or otherwise assign or transfer the Services or any rights thereto in whole or in part
- use the Services to store or transmit infringing, libelous, or otherwise unlawful or taurus material, or to store or transmit material in violation of third-party rights (including privacy rights)
- use the Services to store or transmit Malicious Code
- interfere with or disrupt the integrity or performance of the Services or third-party data contained therein
- attempt to gain unauthorised access to the Services or related systems and/or networks, or
- use the Services in any manner that would cause NormCyber to be in violation of any laws, rulings or regulations

4. 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.

+44 (0) 203 855 6215 | info@normcyber.com | normcyber.com