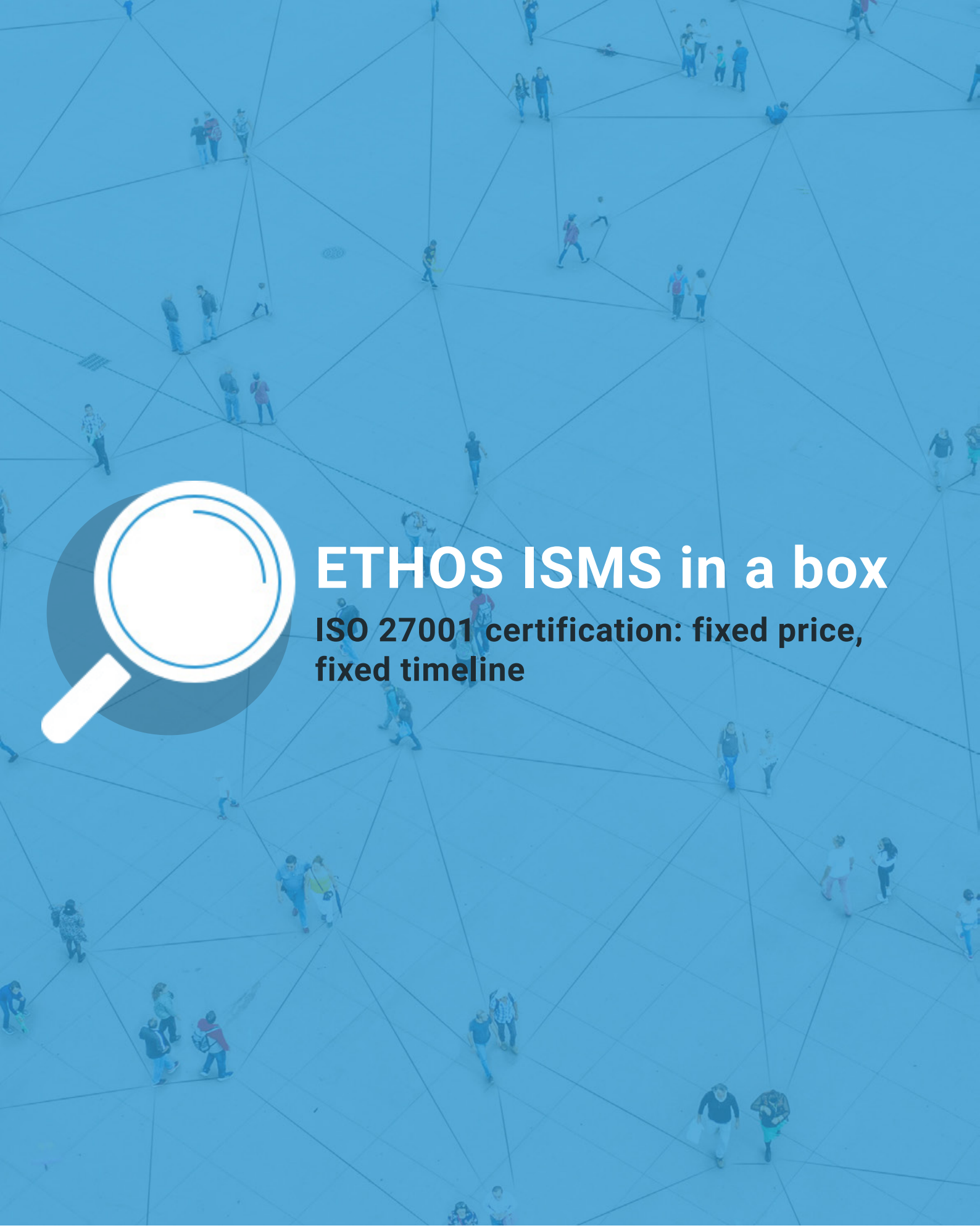

ETHOS ISMS in a box

ISO 27001 certification: fixed price, fixed timeline

ETHOS

ETHOS ISMS in a box

What is Information Security Management System (ISMS) in a box?

- An ISO 27001 gap analysis for your organisation
- A path to certification implementation plan
- Creation of all mandatory documents required to meet the standard (tailored to your business)
- Creation of all mandatory records required to meet the standard (tailored to your business)
- Creation of the non-mandatory documents to support the Annex A controls your business needs
- A professional handover of the ISMS when it is complete
- Employee awareness training so they can operate and maintain the ISMS once certification has been acquired
- Support during your ISO 27001 independent assessment

What will it cost me and how long will it take?

30 days of ETHOS effort over a 3-month, elapsed implementation period. This is a fixed cost.

Our experience enables us to implement your ISMS within the 30 days ETHOS period. There are no hidden charges and we do not only, remain engaged until you have gained your certification, but we also ensure your staff have the knowledge to operate and maintain the ISMS once the work package is complete.

Why ETHOS?

Many organisations know they need ISO 27001 certification, but do not have the time and resources readily available to undertake the compliance work their business needs to gain the certification.

No problem, ETHOS has an ISMS in box just for you.

At ETHOS we will build your ISMS from the bottom up, including:

- Documenting the necessary policies and procedures
- Generating mandatory evidence records
- Creating a staff handbook and guidance
- Business management manual
- Statement of applicability
- Information risk assessment
- Other documentation necessary to deliver the effectiveness of the information security management system.

ETHOS

ETHOS has subject matter experts who can apply their vast knowledge and experience to your business, defining and then implementing the transition to an ISO 27001 compliant operation, on your behalf.

Need the detail?

The organisation's information security management system shall include:

a. Documented information required by this International Standard; and

b. Documented information determined by the organization as being necessary for the effectiveness of the information security management system. (Reference: ISO/IEC 27002:2013)

Mandatory documentation set for an ISO 27001 ISMS

- Scope of the ISMS (clause 4.3)
- Information security policy and objectives (clauses 5.2 and 6.2)
- Risk assessment and risk treatment methodology (clause 6.1.2)
- Statement of Applicability (clause 6.1.3 d)
- Risk treatment plan (clauses 6.1.3 e and 6.2)
- Risk assessment report (clause 8.2)
- Definition of security roles and responsibilities (A.7.1.2 and A.13.2.4)
- Inventory of assets (A.8.1.1)
- Acceptable use of assets (A.8.1.3)
- Access control policy (A.9.1.1)
- Operating procedures for IT management (A.12.1.1)
- Secure system engineering principles (A.14.2.5)

(Note that documents from this standard Annex A, are mandatory only if there are risks which would require their implementation).

Mandatory record set for an ISO 27001 ISMS

- Records of training, skills, experience, and qualifications (clause 7.2)
- Monitoring and measurement results (clause 9.1)
- Internal audit program (clause 9.2)
- Results of internal audits (clause 9.2)
- Results of the management review (clause 9.3)
- Results of corrective actions (clause 10.1)
- Logs of user activities, exceptions, and security events (A.12.4.1 and A.12.4.3)

Other documentation you might need for your ISO 27001 ISMS:

There are numerous non-mandatory documents that may be necessary for your ISO 27001 implementation, especially for the security controls from Annex A. ETHOS will create these non-mandatory documents as part of your ISMS in a box package, as required.

These might include:

- Procedure for document control (clause 7.5)
- Controls for managing records (clause 7.5)
- Procedure for internal audit (clause 9.2)
- Procedure for corrective action (clause 10.1)
- Bring your own device (BYOD) policy (A.6.2.1)
- Mobile device and teleworking policy (A.6.2.1)
- Information classification policy (A.8.2.1, A.8.2.2, and A.8.2.3)
- Password policy (A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, and A.9.4.3)
- Disposal and destruction policy (A.8.3.2 and A.11.2.7)
- Procedures for working in secure areas (A.11.1.5)
- Clear desk and clear screen policy (A.11.2.9)
- Change management policy (A.12.1.2 and A.14.2.4)
- Backup policy (A.12.3.1)
- Information transfer policy (A.13.2.1, A.13.2.2, and A.13.2.3)
- Business impact analysis (A.17.1.1)
- Exercising and testing plan (A.17.1.3)
- Maintenance and review plan (A.17.1.3)
- Business Continuity Plan (A.17.2.1)

ETHOS is available to answer any questions you may have about the implementation process for ISMS in a box. Feel free to contact us for a fixed price quote and a more detailed explanation of how we intend to approach design and deployment of your ISO 27001 implementation package.

For more information about ETHOS safety and innovation work please find us on:

@LtdETHOS

linkedin.com/company/ethos-ltd

or email us at: info@ethos.co.im