Applying ISO27K to your business

ETHOS Advice & Assistance

ETHOS

Applying ISO27K to your business

ETHOS provides specialist advice and assistance in implementation of the ISO27001/ 27002 standards but also have significant experience with other standards within the 27k family too.

The ISO/IEC 27000-series comprises information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

At ETHOS we find most of our clients are looking for 27001 support.
This ambition tends to fall into one of the following 3 categories:

1. **We need ISO 27001 certification now but we do not have the resources readily available to undertake the implementation.**
   ETHOS offers an Information Security Management System (ISMS) in a box product.

   We build your ISMS from the bottom up for a fixed cost of 30 days effort and implement across your organisation within a 3 months elapsed timeframe. We support the independent assessment which will see that your certification is awarded.

2. **We want to implement ISO 27001, have some of the expertise in-house but need some additional support to complete the process.**
   ETHOS can review your current implementation status, identify any gaps in resource requirements and then support your in-house resources to complete the ISMS setup and get you through the assessment. We can do as little, or as much of the work as you require.

3. **We are already ISO 27001 certified but need some support to maintain compliance of our ISMS and undertake the Internal Audit process.**
   ETHOS can provide either a virtual Compliance Officer or virtual Internal Auditor, starting from just a couple of days effort per month to maintain your ISMS and meet your Internal Audit commitments, saving over-committing to specialist resources, in-house.

It's not just ISO 27001, right?

That is correct. Although ISO 27001 is the most implemented standard, along with the controls from ISO 27002, the 27k family is comprised of many other specialist standards you may consider such as **ISO 27799:2016 - Specifically for Health**.

ISO 27799 applies ISO/IEC 27002 to the healthcare domain in a way that carefully considers the appropriate application of security controls for the purposes of protecting personal health information.

ETHOS recommends certification against ISO 27001, identifying the appropriate controls from ISO 27002 and for businesses to consider the targeted guidance from ISO 27799 during implementation. We available to answer any questions you may have about our ISO 27K services to see how we can best assist you in your ISO 27k journey.

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

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