devoteam
Cyber Trust

Roadmap ISO 27001

Integrity **5-step** approach to 27001

Preparation	1 to 2 months	**1. ISMS Preparation** Establishing the appropriate framework for the business needs and providing the organizations with the required skills.
Diagnosis	1 to 3 months	**2. Diagnosis** To identify, within the defined scope, the maturity of processes, applicable controls, risks and mitigation control. To undersand the business and to determine the gap between the standard requirements and the organisation practice so as to allocate resources for an efficient ISMS implementation.
Implementation	1 to 4 months	**3. ISMS Implementation and documentation** To create the mandatory documentation and to start the risk treatment having the applicable control systems into account.
Operation	3 to 6 months	**4. ISMS Operation** To execute the processes and procedures defined, highlighting the fulfilment of objectives, to identify both opportunities for improvement and nono-conformities and to guarantee that the ISMS may be reviewed by the lead management.
Certification and monitoring	1 month + 3 years	**5. Certification and monitoring** Third-party audits to show the maturity of the ISMS and the reduction of risk according to the defined objectives. ISMS monitoring in the form of implementation and management services (planning, performance evaluation and continuos improvement).

devoteam
Cyber Trust

Roadmap ISO 27001

1. ISMS Preparation | 1 to 2 months

Setting the scope

To characterize the functional units, business processes, geography and assets to be protected.

Specific training in ISO 27001

To provide the project team and all the interested parties with knowledge in ISMS.

Training in information security

To provide the project team with updated knowledge in information security aligned with the present moment.

2. Diagnosis | 1 to 3 months

Specific diagnosis

To understand the business and to determine the gap between the standard requirements and the organization practice so as to allocate resources for an effective and efficient implementation.

Presentation of results

Present to top management and all interested parties with the outcomes of the analysis performed.

Documentating the methodology of risk management

To create a document containing the description of the analysis methodology and risk treatment, identifying the responsibilities, the menace sources and vulnerabilities, the existing control systems and their efficiency, as well as the criteria for risk acceptance.

Risk evaluation

The start of the continued implementation of the risk analysis activities anticipated in the risk management methodology.

Risk tretatment planning

The design of a risk treatment plan according to the methodology of risk management set and adopted.

3. ISMS Implementation and documentation | 1 to 4 months

Defining the in formation security policy

To document the aims of the information security of the organization, as well as the commitment of the lead management with risk reduction and the implications of the non-compliance of the defined policy.

Documenting the ISMS processes

To create documents with the description of processes and the respective responsibilities, identifying the adequate registry and evidence.

Declaration of applicability (SoA)

Creation of a registry containing the information on the applicable control systems, eventual exclusions and the respective justifications.

Documentation approval

Approval, by the lead management, of the ISMS scope, the security policy, risk analysis, the risk treatment plan and the SOA.

4. ISMS Operation | 3 to 6 months

Training and awareness-raising

Planning and implementation of training and awareness-raising sessions for the whole organization in the ISMS scope.

Process management

Continuous implementation of the tasks of the several processes which had been previously defined and documented.

ISMS monitoring

Monitoring and evaluation of ISMS metrics and aims.

ISMS review

Formal revision of ISMS input and output to be done by the lead management in accordance with the standard.

Internal audit

Implementation of a formal action of internal audits, analysing registries and evidence of implementation of the processes defined.

5. Certification and monitoring | 1 month + 3 years

Pre-audit (1 month)

Execution of audit by the certifying entity.

Concession audit (1st year)

Monitoring audit (2nd and 3rd year)

Led by the certifying entity.