devoteam
Cyber Trust

Roadmap ISO 27701

Integrity **5-step** approach to 27701

Preparation	1 month	**1. Preparation** To define the scope adequate to the business needs and to endow the organisation with the necessary knowledge.
Diagnosis	1 to 3 months	**2. Diagnosis** Understand the business and determine the GAP between the requirements of the standard and the organisation's practices in order to allocate resources for an efficient implementation of the PIMS. In the characterized scope, to identify the maturity of processes, applicable controls and mitigation risks and controls.
Implementation	1 to 3 months	**3. Implementation** To elaborate the mandatory documentation and to begin the risk treatment considering the applicable controls.
Operation	3 months	**4. Operation** To execute the defined processes and procedures evidencing the objectives fulfilment, to identify improvement opportunities and non-conformities and to guarantee that the PIMS is reviewed by Top Management.
Certification	1 month	**5. Certification** Audit of 3rd part to demonstrate the maturity of ISMS and risk reduction according to the defined objectives.

devoteam
Cyber Trust

Roadmap ISO 27701

1. Preparation | 1 month

To characterize the scope

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

Specific training in ISO 27701

To endow the project team with knowledge in Privacy Information aligned to the present.

Monthly status points

Updating of project plan, identification of project achievement and eventual identified constraints.

2. Diagnosis | 1 to 3 months

Specific diagnosis

To understand the business and to determine the gap between the standard requirements and the organisation practices in order to allocate resources for an efficient implementation of ISMS.

Presentation of results

To present the conclusions of the performed analysis to the Top Management and all the stakeholders.

To document the risk management methodology

To elaborate a document with the description of risk assessment and treatment methodologies, identifying the responsibilities, threats and vulnerabilities sources, existent controls and their efficacy and the risk acceptance criteria.

Risk assessment

Beginning of the ongoing execution of risk assessment activities planned in the risk management methodology within the scope of the protection of personal data.

Risk tretatment plan

Definition of a risk treatment plan according to the defined and adopted risk management methodology for risks in the field of personal data protection.

Monthly status points

Updating of project plan, identification of project achievement and eventual identified constraints.

3. Implementation | 1 to 3 months

To define privacy information policy

To document organisation's Information Security objectives, the commitment of Top Management with the risk reduction and the implications of the non compliance of the defined policy.

To document PIMS processes

To elaborate documents with processes description, respective responsibilities, identifying the adequate records and evidences.

Statement of applicability (SoA)

Elaboration of a record with the applicable controls information, eventual exclusions and the respective justifications.

Document approval

Approval by the Top Management of the PIMS scope, information security policy, risk analysis, risk treatment plan and SoA.

Monthly status points

Updating of project plan, identification of project achievement and eventual identified constraints.

4. Operation | 3 months

Training and awareness

Planning and execution of training and Awareness actions to all the organisation in the PIMS scope.

Process management

Execution in an ongoing manner of the tasks of the several defined and documented processes.

ISMS monitoring

Follow-up and assessment of PIMS metrics and goals.

Internal audit

Execution of a formal action of internal audit, analysing records and evidences of defined processes execution.

ISMS review

Formal review by Top Management of PIMS inputs and outputs according with the standard.

Monthly status points

Updating of project plan, identification of project achievement and eventual identified constraints.

5. Certification | 1 month

Audit of concession (1st year)

Execution of audit by the certifying entity.

Audit of follow-up (2nd and 3rd year)

Execution of the audit by the certifying entity.

Audit of certification (after 3rd year)

Execution of the audit by the certifying entity.

Maintenance of certification
(tasks out of the project scope)