ISO 27701 – Privacy Information Management system

What is ISO 27701?

ISO 27701 specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization.

It specifies PIMS-related requirements and provides guidance for PII controllers and PII processors holding responsibility and accountability for PII processing.

It applies to all organization's which are PII controllers and/or PII processors processing PII within an ISMS.

Is ISO 27201 a certifiable standard?

It is a " Requirements and Guidelines standard. The requirements are shall statements (there are 67 shall statements in the standard) and it is a certifiable standard.

Can an organization get an ISO 27701:2019 certification without ISO 27001:2013 certification?

No, since this is an extension of ISO 27001 standard it is possible to obtain an ISO 27701 certification only as an extension to ISO 27001 certification?

Is this certification recognized under GDPR Article 42?

No, EU Council has not yet recognized any certification mechanism under GDPR. However, ISO

27701 could be a potential certification mechanism

Has any organization been certified to ISO 27701?

Yes. One Trust is certified to ISO 27701. The certification body is Colafire, a US based certification body.

What should be the duration of the training? Or

Is it essential to do a 5 Day Lead Implementation training for ISO 27701 even if I have undergone an ISO 27001 training in the past?

We foresee 3 scenarios:

1. Undergone an ISO 27001 training as well as GDPR training

2. Undergone an ISO 27001 training alone

3. Undergone a GDPR training alone or not undergone any of the two trainings

We respect your time and your existing knowledge.

The duration of our training is as follows:

Scenario 1 – a two training on integration of ISO 27001 with the GDPR focusing on

implementing an ISMS for Privacy Information Management System for PII.

Scenario 2 – a three day training focusing on aspects related to GDPR implementation from the standpoint of Controller and processor and extending ISO 27001 to include PIMS.

Scenario 3 – a five days training focusing on Management system, implementing Information Security Management system and Privacy Information Management System.

I already have implemented ISO 27001 and also implemented GDPR. What are the steps of implementation of ISO 27701?

1. Senior management training

2. Gap Assessment

3. Enhance and Refine the ISMS Policy, Objectives to include Privacy aspects

4. Define the PIMS Context, interested parties needs

5. Define scope keeping in mind the context of PII data types, Processes and systems which handle PII

6. Refine the criteria for doing Privacy Risk Assessment

7. Conduct the integrated ISMS and PIMS Risk Assessment

8. Define Statement of Applicability including the 21 additional requirements to ISO 27001 Annexure A controls, 31 controls and control objectives of Annexure A 277701 for cases where you are a Controller and 18 cases where you are a processor.

9. Implement Privacy by Design

10. Implement necessary policies and Procedures such as Data Subject Rights and Breach handling.

11. Implement necessary technical and organizational measures

12. Conduct Internal auditor trainings of PIMS

13. Conduct internal audits if PIMS

14. Apply for Certification

I already have implemented ISO 27001. However, I am yet to implement GDPR

What are the steps of implementation of ISO 27701?

In addition to the steps above activities such as Data Discovery, Data Inventory, Data Flows, Records of Processing Activities, Data Protection Organization structure such as DPOs and others, Data Protection Impct Assessment, putting in place an Accountability Framework also needs to be done.

Implementing ISO 27701: 2019 PIMS – Two Common Fallacies

This article covers two common implementation aspects of ISO 27701 which may be ignored by practitioners/consultants.

Implementation of ISO 27701:2019 – Importance of Annex F and two of the referenced standards (ISO 20889 and ISO 19944)

Fallacy #1 – Implement Annexure A of ISO 27701 if you are a controller or Annexure B of ISO 27701 and you have implemented ISO 27701

Very often I encounter people who think that implementing Annex A and Annex B of ISO 27701 will result in implementation of PIMS. These are the people who can not comprehend how this standard can be used for implementing a Privacy Information Management System Framework and hence this mistake.