Deming Certification & Rating Pvt. Ltd.

Email: - info@demingcert.com
Contact: - 02502341257/9322728183
Website: - www.demingcert.com
No. 108, Mehta Chambers, Station Road, Novghar, Behind Tungareswar Sweet,
Vasai West, Thane District, Mumbai- 401202, Maharashtra, India

AIOTA Certification

What is AIOTA Certificate?

The design goal is to enhance the existing Information Security Management System (ISMS) with additional requirements in order to establish, implement, maintain, and continually improve a Privacy Information Management System (PIMS). The standard outlines a framework for Personally Identifiable Information (PII) Controllers and PII Processors to manage privacy controls to reduce the risk to the privacy rights of individuals.

ISO/IEC 27701 is intended to be a certifiable extension to ISO/IEC 27001 certifications. In other words, organizations planning to seek an ISO/IEC 27701 certification will also need to have an ISO/IEC 27001 certification.

Intended application of the standard

The intended application of ISO/IEC 27701 is to augment the existing ISMS with privacy-specific controls and, thus, create PIMS to enable effective privacy management within an organization.

A robust PIMS has many potential benefits for PII Controllers and PII Processors, with at least three significant advantages:

First, achieving compliance to privacy requirements (particularly laws and regulations, plus agreements with third parties, plus corporate privacy policies etc.) is burdensome, especially if the requirements are not organized in the most effective way for PII Controllers and PII Processors. Organizations subject to multiple privacy compliance obligations (e.g. from several jurisdictions in which they operate or data subjects live) face additional burdens to reconcile, satisfy and keep watch on all the applicable requirements. A managed approach eases the compliance burden, for example as demonstrated by Annex C of the standard, a single privacy control may satisfy multiple requirements from General Data Protection Regulation (GDPR).

Second, achieving and maintaining compliance with applicable requirements is a governance and assurance issue. Based on the PIMS (and, potentially, its certification), Privacy or Data Protection Officers can provide the necessary evidence to assure stakeholders such as senior management, owners and the authorities that applicable privacy requirements are satisfied.

Third, PIMS certification can be valuable in communicating privacy compliance to customers and partners. PII Controllers generally demand evidence from PII Processors that the PII Processors' privacy management system adheres to applicable privacy requirements. A uniform evidence framework based on international standard can greatly simplify such communication of compliance transparency, especially when the evidence is validated by an accredited third-party auditor.[4] This necessity in communication of compliance transparency is also critical for strategic business decisions such as mergers and acquisitions and co-Controllers scenarios involving data sharing agreement. Lastly, PIMS certification can potentially serve to signal trustworthiness to the public.

Normative references

ISO/IEC 27701 normatively references the following documents:

- ISO/IEC 27001
- ISO/IEC 27002:2017-06

Structure of the standard

The requirements of the standard are segregated into the four following groups:

1. PIMS requirements related to ISO/IEC 27001 are outlined in clause 5.
2. PIMS requirements related to ISO/IEC 27002 are outlined in clause 6.
3. PIMS guidance for PII Controllers are outlined in clause 7.
4. PIMS guidance for PII Processors are outlined in clause 8.

The standard further includes the following Annexes:

1. Annex A PIMS-specific reference control objectives and controls (PII Controllers)
2. Annex B PIMS-specific reference control objectives and controls (PII Processors)
3. Annex C Mapping to ISO/IEC 29100
4. Annex D Mapping to the General Data Protection Regulation (GDPR).
5. Annex E Mapping to ISO/IEC 27018 and ISO/IEC 29151
6. Annex F How to apply ISO/IEC 27701 to ISO/IEC 27001 and ISO/IEC 27002

History of the standard

A new work item was proposed to JTC 1/SC 27 by JTC 1/SC 27/WG 5 "Identity management and privacy technologies" in April 2016 based on an initiative by experts from the French National Body of JTC 1/SC 27.

The project was then developed in JTC 1/SC 27/WG 5 under the number ISO/IEC 27552.

British Standards Institution (BSI) made the first CD of ISO/IEC 27552 publicly available from its web store in February 2018.

The second CD of ISO/IEC 27552 was published in August 2018.

The DIS of ISO/IEC 27552 was issued in January 2019 and approved in March 2019. As no technical changes were necessary, the FDIS ballot was bypassed.

ISO/IEC JTC 1/SC 27 completed the technical work on ISO/IEC 27552 in April 2019.

Before its publication, ISO/IEC 27552 was renumbered to ISO/IEC 27701 as per the Resolution 39/2019 of ISO/Technical Management Board, which mandates that any Management System "type

A" (containing requirements) shall have a number finishing with “01” as its last two digits. The renumbering was finalized in July 2019.

The standard was published on August 6th, 2019.