schellman
Quality. above all.

The Much Anticipated **ISO/IEC 27701:2019**

For those that were monitoring the wire, ISO/IEC 27001:2019 (ISO 27701) was released the week of August 5th. In draft form, it was previously labeled ISO/IEC 27552 (should you be wondering why that specific standard number has not been issued). You can obtain a copy of the published version here: www.iso.org/standard/71670.html.

WHITEPAPER

schellman
Quality. above all.

What is the Objective?

There has been much market anticipation for this standard to be released. It is titled *Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management – Requirements and Guidelines.* The objective is to provide organizations additional requirements and guidance, specific to elements of the information security management system (ISMS) as well as for additional control guidance and implementation requirements for controls noted within Annex A (and considerations of those from ISO/IEC 27018 and ISO/IEC 29100) that would support an effective privacy information management system (PIMS) as an extension to an organization's ISMS. The beauty of ISO 27701 is that it is intended to be applicable to any organization that would be considered a controller or processor for personally identifiable information (PII) in the context of their ISMS.

WHITEPAPER

The Structure of ISO 27701

The structure of the standard is broken down by clauses, where each provides additional requirements or implementation guidance on 1) necessary modifications to the ISMS (Clause 5), 2) additional information security controls (Clause 6), 3) additional controls for PII controllers (Clause 7), and 4) additional controls for PII processors (Clause 8). The standard also includes six Annexes which cover:

- ***Annex A*** – PIMS-specific control objectives and controls for an organization acting as a PII controller
- ***Annex B*** – PIMS-specific control objectives and controls for an organization acting as a PII processor
- ***Annex C*** – Mapping to ISO/IEC 29100
- ***Annex D*** – Mapping of the controls in ISO 27701 to the European Union General Data Protection Regulation (GDPR)
- ***Annex E*** – Mapping to ISO/IEC 27018 and ISO/IEC 29151
- ***Annex F*** – Explanation on how ISO/IEC 27001 and ISO/IEC 27002 are extended to the protection of privacy when processing PII.

WHITEPAPER

schellman
Quality. above all.

How Would an Organization Approach 27701

As extensions to the ISMS go, ISO 27701 is a much bigger task for organizations that may have previously included ISO/IEC 27017 or ISO/IEC 27018 into their management systems. The effort must consider key modifications to the overall ISMS structure and requirements, modification of existing controls from Annex A, as well as the implementation of the control objectives and controls that may be relevant to either a PII processor or PII controller. For organizations that may have a structure and processes in place to support the requirements of GDPR, the transition to conform to ISO 27701 may be a bit simpler; however, the need is still to ensure that these processes are effectively implemented into the scope of the ISMS.

For any scope modification, including incorporating ISO 27701 into your ISMS, there are some necessary tasks to complete.

- ***Perform a gap assessment*** of your existing ISMS to the requirements of ISO 27701.
- ***Assign owners to identified gaps*** and produce an action plan as to how to address those gaps.
- ***Revise the design of the ISMS*** to incorporate these new requirements.
- ***Perform the necessary activities*** on the revised ISMS, including but not limited to the risk assessment, measurement and monitoring, internal audit, management review.
- ***Assess the output from the operations*** of the revised ISMS to ensure that it meets the existing and net-new requirements and that any areas of deficiency or nonconformance are processed through the formalized continual improvement or corrective action process.

WHITEPAPER

schellman
Quality. above all.

How Soon Can I Implement ISO 27701?

With the release of this standard being relatively new to the market, there will be those early adopters and market drivers. However, it is important to note that with the criticality of the objective of this standard, ISO is looking to identify specific requirements, both in competency and in process, for certification bodies to adhere to when effectively performing an audit against ISO 27701. These pending new requirements may necessitate certification bodies to modify their existing methodology and approach related to ISO 27701 assessments, which could lengthen the timeline for when an external audit could be properly performed. If new requirements are issued, it may allow for additional time for most organizations to appropriately implement ISO 27701 into their ISMS.

Schellman will continue to monitor any updates and will be sure to communicate them as they unfold. Additionally, we plan to provide a detailed guide to ISO 27701 that will be coming in the next month to help organizations better understand the approach and requirements of ISO 27701.

For more information or to request a consultation, please visit www.schellman.com/iso-certifications

Speak with a Cybersecurity specialist about your organization's information security needs today.

CLICK FOR MORE INFO

schellman
Quality, above all.

www.schellman.com
4010 W Boy Scout Blvd, Suite 600
Tampa, FL 33607
1.866.254.0000

Outside of the United States,
please dial: +1.973.854.4684