Technical Bulletin – Guidance on applying for an Extension to Scope for ISO/IEC 27701:2019, Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management

03 March 2020

Overview

This Technical Bulletin is applicable to all Information Security Management Systems (ISMS) Certification Bodies.

ISO/IEC 27701:2019, initially developed as ISO/IEC 27552, specifies the 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 an organisation.

Following the publication of ISO/IEC 27701:2019, this bulletin has been produced to update certification bodies and stakeholders on the proposed approach for extending accreditation for this new standard.

This new standard is considered to be an Information security management system (ISMS) sector-specific document and extends the requirements of ISO/IEC 27001:2013 to take into account the protection of privacy of Personally Identifiable Information (PII) principals as potentially affected by the processing of PII, in addition to information security.

Following the publication of ISO/IEC 27701:2019 on 05 August 2019, this technical bulletin outlines the assessment process for all currently accredited ISMS certification bodies wishing to make an application to extend their ISO/IEC 27001:2013 accreditation to include ISO/IEC 27701:2019.

All certification bodies wishing to extend their current scope to include ISO/IEC 27701:2019 must submit documentary evidence supporting their approach to implementing the requirements of the new standard. For this a completed AC1 application form will be required.

The documentary evidence shall include:

a. a fully documented gap analysis of the Operational differences, as identified by the CB, between the currently accredited ISO/IEC 27001:2013 certification being offered by the certification body and the new extension standard ISO/IEC 27701:2019;
b. the gap analysis shall identify the impact of the anticipated changes to their certification activity and the actions to be undertaken to ensure effective certification when incorporating the new standard in their ISMS Scheme offering;
c. a detailed implementation plan to address the required changes for all activities as identified in the gap analysis, including how the CB will be 'rolling out' the new certification programme for clients;
d. a list of all current auditors for ISO/IEC 27001:2013 in the certification team and indicate those who have successfully completed any ISO/IEC 27701:2019 update training along with evidence to support that training. The applicant shall also indicate when it is intended for any remaining auditors,

and other certification personnel, (contract reviewers, technical reviewers and decision makers) to complete the training for the new standard.

The application and accompanying documentation shall be submitted to:

The Applications Unit
United Kingdom Accreditation Service
2 Pine Trees, Chertsey Lane,
Staines-upon-Thames,
Middlesex,
TW18 3HR

or Email: apps@ukas.com

It is anticipated that UKAS will be able to offer assessments for the new standard, ISO/IEC 27701:2019, from 31 March 2020.

The Assessment Process

The UKAS assessment for this extension to scope will comprise the following activities:

i. a remote desktop assessment of all the documentation submitted to determine apparent readiness of the organisation to implement the new standard and to inform the head office assessment for ISO/IEC 27701:2019;

ii. a head office assessment for ISO/IEC 27701:2019 to include review and verification of the process of administration of the requirements, and technical competence for personnel;

iii. a witnessed assessment for ISO/IEC 27701:2019, selected by UKAS, will be required before the scope of accreditation can be extended for the new standard.

The UKAS assessment for ISO/IEC 27701:2019 is not anticipated to be a complicated activity. Depending on the specific operational and geographical context of the certification body, the following effort is envisaged:

Assessment Component	Estimated Office Effort (days)	Estimated Site Effort (days)
Remote desktop assessment	1.50	0.00
Head office assessment	1.50	2.00 – 4.00
Witnessed assessment	1.00	*audit duration*

Both office and site effort will be chargeable at the standard UKAS day rate. Additional effort will be needed if improvement actions are identified that will need to be reviewed and verified to support the extension decision. Any further effort in the visit programme for the extension will be dependent on the outcomes of the documentation review, office assessment and witness.

CBs will be individually informed of estimated costs to your business at the time of the assessment work being booked. You will be informed of any improvement actions in the usual assessment report format. These will need to be resolved satisfactorily through the UKAS corrective action process before any extension of your scope of accreditation can be made.

Should you require any clarification on the above, please contact your Assessment Manager; Alastair Hunter: Technical Focus Person (Information Assurance) – alastair.hunter@ukas.com; or Kevin Belson: Technical Manager - Kevin.Belson@ukas.com