Technical Bulletin: Transition arrangements for ISO/IEC 27001:2022

19 December 2022

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

Following the publication of ISO/IEC 27001:2022, this bulletin has been produced to update Certification Bodies and stakeholders on the UKAS assessment process and overall timelines for assessment against the requirements of the revised certification standard.

Compared to the previous version (edition 2), the revised edition has revised the notes of 6.1.3c), 6.1.3 d) and Annex A has been aligned with the controls defined in ISO/IEC 27002:2022, which contains 93 controls (11 of which are new) organised in 4 themes. In addition to the 11 new controls, 24 have been merged and 58 have been updated.

At time of writing, UKAS understand that the IAF aims to publish an updated transition instruction (IAF MD 26, Issue 2.0) imminently. This will require Accreditation Bodies to be ready to conduct assessments within 6 months following publication of the revision, and that Accreditation Bodies shall complete the transition of all Certification Bodies within 12 months following the publication date.

To enable the transition to progress in a timely manner, Certification Bodies are requested to complete a documented gap analysis detailing how they have implemented the changes introduced by ISO/IEC 27001:2022 and forward it to UKAS by no later than **31 March 2023**. The submitted information shall include:

+ the gap analysis of the changes in ISO/IEC 27001:2022

+ the transition arrangements and evidence of implementation

+ evidence of the authorisation of related personnel

Given the limited number of changes introduced by ISO/IEC 27001:2022, it is not envisaged that significant additional assessment effort will be required by UKAS to review the changes made by the certification body, however this is dependent on the clarity of the submitted information provided by the CB. It is estimated that an initial 1.00 day of effort will be required to review the changes and complete the associated back-office activities.

If the initial technical document review is unable to verify the effective implementation and conformance with the Certification Body's transition arrangements, then an office assessment may be required. If areas are identified that do not adequately fulfil the revised requirements, then these will be raised as findings. All mandatory findings shall be addressed by the Certification Body in the normal way.

Timeline:

Date	Milestone/Activity
25 October 2022	Publication of ISO/IEC 27001:2022
30 April 2023	UKAS ready to assess to ISO/IEC 27001:2022
31 October 2023	All UKAS transitions of CB's completed
31 October 2023	All initial certifications by CB to be completed against ISO/IEC 27001:2022 from this date
31 October 2025	All CB transitions of clients completed

Should you require any clarification on the above, please contact your Assessment Manager in the first instance. In the absence of your Assessment Manager, one of the following may be able to assist:

+ Kevin Belson: Technical Manager – kevin.belson@ukas.com
+ Alastair Hunter: Technical Focus ISMS – alastair.hunter@ukas.com
+ Steve Randall: Technical Focus ISO/IEC 17021-1 – steve.randall@ukas.com

UKAS