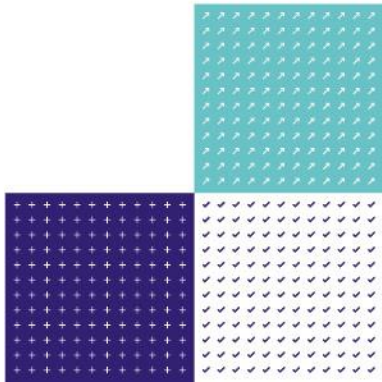
UKAS
A world of confidence

CIS 16

Edition 2 November 2020

UKAS Requirements for ISMS Certification Bodies Certifying Privacy against ISO/IEC 27701:2019



Contents

Changes since last edition

The reference to the Information Commissioners Office (ICO) has been removed from Paragraph 1.4.

1. Introduction

1.1 This document sets out the background to the UKAS assessment and accreditation of ISMS Certification Bodies who wish to be accredited for the provision of certification against the privacy information management requirements of ISO/IEC 27701:2019. It defines the requirements to help UKAS ensure consistency of application when considering the competence, impartiality and integrity of ISMS certification body's offering the extended scope of privacy management.

1.2 Due to the increasing number of information and communication technologies (ICT) that process personally identifiable information (PII), it is important to have international information security standards that provide a common understanding for the protection of PII. Protection of privacy in the context of the processing of PII is a societal need, as well as the topic of dedicated legislation and/or regulation all over the world.

1.3 It is important that UKAS, in its capacity as the UK's National Accreditation Body, responds to market needs for the protection of privacy by determining, in the public interest, the technical competence and integrity of certification bodies providing assurance to the market, regarding the processing and protection of PII.

1.4 As ISO/IEC 27701 relates to personally identifiable information, there is a mapping (in Annex D) to the EU GDPR (General Data Protection Regulation). Please note that accredited certification for the GDPR shall be based on accreditation to ISO/IEC 17065 using a certification scheme approved by the Supervisory Authority in an EU Member State (see GDPR, Articles 42 and 43). Accredited certification of a management system that includes the additional requirements of ISO/IEC 27701 under ISO/IEC 17021-1 would not meet these criteria. ISMS Certification Bodies shall ensure their clients are aware of this distinction and that those clients remain responsible for assessing their legal obligations and deciding how to comply with them.

2. Background

2.1 Compliance with the privacy information management requirements in ISO/IEC 27701:2019 is based on adherence to the requirements defined in ISO/IEC 27001:2013. It is considered to extend the requirements of ISO/IEC 27001:2013 to take into account the protection of privacy of PII principals potentially affected by the processing of PII, in addition to information security. It is considered to be a sector-specific document supporting ISO/IEC 27001:2013.

2.2 To support the accreditation of certification bodies providing ISMS certification, the international standards community has specified requirements and provided guidance for bodies providing audit and certification of an information security management system (ISMS). These requirements are defined in ISO/IEC 27006 and are in addition to the requirements contained within ISO/IEC 17021-1 and ISO/IEC 27001.

2.3 In the event that the international standards community subsequently publishes a set of accreditation requirements to support the implementation of ISO/IEC 27701:2019 then such requirements shall take precedence over those defined in the present document until it is either revised or withdrawn.

3. Scope of Accreditation

3.1 The scope of UKAS accreditation is the certification of an information security management system that takes into account the protection of privacy of PII principals affected by the processing of PII. The criteria used by UKAS for accreditation is ISO/IEC 17021-1 as supplemented by ISO/IEC 27006, where the requirements of ISO/IEC 27006 mentioning “information security” shall be extended to the protection of privacy as potentially affected by the processing of PII. Therefore, in practice, this means that where "information security" is used in ISO/IEC 27006, "information security and privacy" shall apply instead, unless otherwise stated in this document.

3.2 The UKAS Management Systems Accreditation Schedule will reference the new ISO/IEC 27701 standard as a Sector Scheme and will appear on the schedule, within the information security management system section, as follows:

> **Information Security Sector Schemes**
>
> **Privacy Information Management**
> ISO/IEC 27701:2019

3.3 The accreditation schedule will also include geographical scoping. The certification body will need to demonstrate knowledge and awareness of privacy risks and controls associated with the geographical locations within its scope of accreditation.

4. Application for extension to ISMS Scope of Accreditation

4.1 All ISMS 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 which is available on the UKAS website.

4.2 The documentary evidence shall include:

- 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;
- 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, and the requirements defined in this document, in their ISMS Scheme offering;
- 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;
- as part of the above, information on how technical competence criteria have been defined and implemented for ISO/IEC 27701:2019, with evidence of any upskilling required.

The application and accompanying documentation shall be submitted to the applications unit at UKAS via email (apps@ukas.com). Please ensure you cc your Assessment Manager when you apply so they can help track and progress your application smoothly.

5. Assessment Criteria

5.1 The following criteria shall be used for assessment of ISMS certification bodies certifying the information security management systems of organisations taking into account the protection of privacy of PII principals potentially affected by the processing of PII.

- ISO/IEC 17021-1 *Conformity assessment - Requirements for bodies providing audit and certification of management systems Part 1: Requirements*
- ISO/IEC 27006 *Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems*
- ISO/IEC 27701 *Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines*
- ISO/IEC 27000 *Information technology - Security techniques - Information security management systems - Overview and vocabulary*

6. Assessment Approach

6.1 As ISO/IEC 27701 is considered an extension to the information security management systems standard, ISO/IEC 27001, and will be treated as a sector scheme operating within it, certification bodies will have to hold accreditation for ISO/IEC 17021-1, as supplemented by ISO/IEC 27006, for the technical scope of certifying information security management systems ***before*** they can apply to add the privacy information management sector scheme to their accredited scope.

6.2 Assessment shall follow the normal UKAS process as detailed in UKAS publication GEN 1 *General Principles for the Assessment of Conformity Assessment Bodies by the United Kingdom Accreditation Service*.

6.3 The assessment will aim to confirm that the ISMS Certification Body has the necessary competence to carry out effective audits against the extended requirements defined in ISO/IEC 27701 and that systems have been effectively implemented in accordance with ISO/IEC 17021-1 and ISO/IEC 27006, when modified as described in paragraph 3.1 above.

6.4 The UKAS assessment for the extended privacy requirements defined in ISO/IEC 27701 will comprise the following activities:

- 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;
- 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;
- 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.

6.5 Depending on the specific operational and geographical context of the certification body, the following effort is generally envisaged (this is intended as a guide only):

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

IMPORTANT NOTE: Travel and subsistence will apply in line with published UKAS policy, available from our website.

6.6 Both office and site effort will be chargeable at the standard UKAS day rate. Additional effort may 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.

6.7 ISMS Certification Bodies 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.

7. Competence of Personnel

Generic Competence Requirements

7.1 The ISMS certification body shall ensure that it has knowledge of the technological, legal and regulatory developments relevant to the privacy information management systems of the client which it assesses.

7.2 The ISMS certification body shall define the competence requirements for each certification function as referenced in Table A.1 of ISO/IEC 17021-1. The certification body shall take into account all the requirements specified in ISO/IEC 17021-1, ISO/IEC 27006 and this document that are relevant for the technical areas as determined by the certification body.

Determination of Competence Criteria

7.3 The ISMS certification body shall have criteria for verifying the background experience, specific training or briefing of audit team members that ensures at least:

a) knowledge of privacy information management;

b) technical knowledge of the activity to be audited;

c) knowledge of the roles of PII principals, controllers, processors and third parties and how PII may flow amongst them;

d) ability to recognise PII and determine whether or not a natural person could be considered identifiable;

e) knowledge of the different factors that can influence the privacy safeguarding requirements that are relevant to the privacy information management systems of the client which it assesses.

7.4 These above requirements a) to e) apply to all auditors being part of the audit team, with the exception of b), which can be shared among auditors being part of the audit team.

7.5 The audit team shall be competent to trace indications of information security and privacy incidents in the client's management system back to the appropriate elements of the management system.

7.6 The audit team shall have appropriate work experience of the items above and practical application of these items (this does not mean that an auditor needs a complete range of experience of all areas of information security and privacy information management, but the audit team as a whole shall have enough appreciation and experience to cover the scope of the management system being audited).

7.7 Collectively, all members of the audit team shall have knowledge of:

a) information security and privacy specific documentation structures, hierarchy and interrelationships;

b) information security and privacy information management related tools, methods, techniques and their application;

c) information security and privacy risk assessment and risk management;

d) processes applicable to information security and privacy information management;

e) the current technology where safeguarding information security and privacy information may be relevant or an issue.

Every auditor shall fulfil a), c) and d).

7.8 Auditors involved in auditing information security and privacy management systems shall have knowledge of:

a) all requirements contained in ISO/IEC 27001;

b) all requirements contained in ISO/IEC 27701;

c) privacy information management best practices and privacy safeguarding procedures;

d) policies and business requirements for privacy management;

e) information security and privacy risks related to business sector.

Collectively, all members of the audit team shall have knowledge of:

f) all controls contained in ISO/IEC 27002 (if determined as necessary) and their implementation; and

g) the additional or modified control objectives and controls in ISO/IEC 27701 (if determined as necessary) and their implementation;

h) the legal and regulatory requirements in the particular information security and privacy field, geography and jurisdiction(s) within the scope of the management system being audited.

7.9 Personnel conducting the application review to determine audit team competence required, to select the audit team members and to determine the audit time shall have knowledge of:

a) relevant information security and privacy standards and other normative documents used in the certification process;

b) generic terminology, processes, technologies and risks related to the client business sector;

c) client products, processes, organisation types, size, governance, structure, functions and relationships on development and implementation of the information security and privacy management systems and certification activities, including outsourcing functions.

7.10 The personnel reviewing audit reports and making certification decisions shall have knowledge that enables them to verify the appropriateness of the scope of certification as well as changes to the scope and their impact on the effectiveness of the audit, in particular the continuing validity of the identification of interfaces and dependencies and the associated risks. They shall also have knowledge of:

a) information security and privacy specific documentation structures, hierarchy and interrelationships;

b) information security and privacy risk assessment and risk management;

c) processes applicable to privacy information management;

d) legal and regulatory requirements relevant to information security and privacy information management;

e) relevant information security and privacy standards and other normative documents used in the certification process.

Demonstration of Auditor Knowledge and Experience

7.11 The ISMS certification body shall demonstrate that the auditors have knowledge and experience through:

a) recognised information security and privacy management specific qualifications (where privacy management and the safeguarding of personally identifiable information (PII) has been a defined part of that qualification);

b) participation in privacy related training courses and attainment of relevant personal credentials;

c) up to date professional development records;

d) ISMS audits extended by ISO/IEC 27701 and witnessed by another auditor, technically competent for the scope being audited;

e) has professional education or training to an equivalent level of university education;

f) has at least four years full time practical workplace experience in information and communication technology, of which at least two years are in a role or function relating to information security and the safeguarding of personally identifiable information;

g) has successfully completed at least five days of training, the scope of which covers ISMS audits and audit management with at least two days focussed specifically on privacy information management and the safeguarding of personally identifiable information;

h) has gained experience of auditing information and security and privacy prior to acting as an auditor performing audits against the extended requirements of ISO/IEC 27701. This experience shall be gained by performing as an auditor-in-training monitored by an information security and privacy evaluator that is competent to take over the duties and have final responsibility for the activities and findings of the auditor-in-training. The experience shall include participation in at least one information security and privacy initial certification audit (stage 1 and stage 2) or re-certification and at least one surveillance audit. This experience shall be gained in at least 10 onsite audits days of information security and privacy management systems and shall be performed in the last 5 years. The participation shall include review of documentation and risk assessment, implementation assessment and audit reporting;

i) has relevant and current experience;

j) keeps current knowledge and skills in privacy management and the safeguarding of personally identifiable information up to date through continual professional development.

k) has competence in auditing a management system in accordance with ISO/IEC 27001, as extended by ISO/IEC 27701.

Technical experts shall comply with criteria e), f) and i).

7.12 Technical experts shall work under the supervision of an auditor.

8. Confidentiality and Impartiality

8.1 In order to gain access to commercially privileged information, the certification body shall undertake (in a legally enforceable contract) to hold confidential any sensitive, proprietary and or vulnerability information it acquires during an audit. This shall be with due regard to any legislative provisions in place to safeguard personally identifiable information.

8.2 The ISMS certification body shall demonstrate how observations and conclusions on personally identifiable information within auditor notes, reporting documents and other supporting audit records is maintained in confidence.

8.3 The ISMS certification body may add value during certification audits and surveillance visits that consider privacy, e.g. by identifying opportunities for improvement, as they become evident during the audit providing that specific solutions are not recommended. The certification body shall ensure that such added value does not give rise to potential conflicts of interest or create a situation that could reasonably be interpreted as participation in the establishment, implementation or maintenance of the management system subject to certification audit.

8.4 The ISMS certification body shall not provide internal information security or privacy reviews (including privacy impact assessments) of a client's management system subject to certification. Furthermore, the certification body shall be independent from the body or bodies (including any individuals) which undertake internal audit of a client's management system subject to certification.

8.5 Before the certification audit, the certification body shall ask the client to report if any information security or privacy related information (such as records or information about design and effectiveness of controls) cannot be made available for review by the audit team because it contains confidential or sensitive information. The certification body shall determine whether the management system can be adequately audited in the absence of such information. If the certification body concludes that it is not possible to adequately audit the management system without reviewing the identified confidential or sensitive information, it shall advise the client that the certification audit cannot take place until appropriate access arrangements are granted.

8.6 A certification body shall not certify another certification body's ISMS client for a scope of certification limited to only those requirements defined in ISO/IEC 27701. It is considered that as ISO/IEC 27701 extends the requirements of ISO/IEC 27001 then the 2 standards shall be audited together.

9. Scope of Certification

9.1 The audit team shall audit the information security and privacy management system of the client covered by the defined scope against all applicable certification requirements. The certification body audit shall confirm, in the scope of the client's management system, that clients have determined the boundaries and applicability of the management system to establish its scope by considering:

a) external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its management system;

b) interested parties that are relevant to the management system;

c) the requirements of these interested parties relevant to information security and privacy; and

d) interfaces and dependencies between activities performed by the organisation subject to audit, and those that are performed by other organisations.

9.2 The scope of certification shall be clear and unambiguous. the scope shall clearly state what type of PII is processed (processor or controller). Where the client organisation is both a PII processor and

PII controller, the certification body shall ensure that the scope reflects this clearly (i.e. the scope of certification shall not limit the boundary to just the PII processor or PII controller roles).

9.3 Certification bodies shall ensure that the client's information security and privacy risk assessment(s) and risk treatment(s) properly reflect its activities and extends to the boundaries of its activities as defined in the scope of certification. Certification bodies shall confirm that this is reflected in the client's scope of their information security and privacy management system and Statement of Applicability. The certification body shall verify that there is at least one Statement of Applicability per scope of certification.

9.4 Certification bodies shall ensure that interfaces with services or activities that are not completely within the scope of the management system are addressed within the management system subject to certification and are included in the client's information security and privacy risk assessment(s). An example of such a situation is the sharing of facilities (e.g. IT systems, databases and telecommunication systems or the outsourcing of a business function) with other organisations.

9.5 Where applications are received for expanding the scope of an existing ISMS certification to include the protection of privacy of PII principals potentially affected by the processing of PII, the certification body shall undertake a review of the application and determine the additional audit activities necessary to evaluate the implementation, including effectiveness, of the additional requirements defined in ISO/IEC 27701. These additional audit activities may be conducted in conjunction with a surveillance audit.

10. Audit Time Determination

10.1 In addition to the requirements of ISO/IEC 17021-1, 9.1.4 certification bodies shall allow auditors sufficient time to undertake all activities relating to an initial audit, surveillance audit or re-certification audit. The calculation of overall audit time shall include sufficient time for audit reporting. The certification body shall use ISO/IEC 27006 Annex B to determine audit time, supplementing the audit time chart in Table B.1 with the one below.

Number of persons doing work under the organisation's control	ISMS audit time for initial audit (auditor days)	Additional initial audit time for PII Controllers (auditor days)	Additional initial audit time for PII Processors (auditor days)	Additive and subtractive factors	Total audit time
1~10	5.00	1.25	0.75	See B.3.4*	
11~15	6.00	1.75	1.00	See B.3.4*	
16~25	7.00	2.00	1.00	See B.3.4*	
26~45	8.50	2.25	1.25	See B.3.4*	
46~65	10.00	2.75	1.50	See B.3.4*	
66~85	11.00	3.00	1.75	See B.3.4*	
86~125	12.00	3.25	2.00	See B.3.4*	
126~175	13.00	3.50	2.00	See B.3.4*	
176~275	14.00	3.75	2.25	See B.3.4*	
276~425	15.00	4.00	2.25	See B.3.4*	
426~625	16.50	4.50	2.50	See B.3.4*	
626~875	17.50	4.75	2.75	See B.3.4*	
876~1175	18.50	5.00	3.00	See B.3.4*	
1176~1550	19.50	5.25	3.00	See B.3.4*	
1551~2025	21.00	5.75	3.25	See B.3.4*	

Number of persons doing work under the organisation's control	ISMS audit time for initial audit (auditor days)	Additional initial audit time for PII Controllers (auditor days)	Additional initial audit time for PII Processors (auditor days)	Additive and subtractive factors	Total audit time
2026~2675	22.00	6.00	3.50	See B.3.4*	
2676~3450	23.00	6.25	3.75	See B.3.4*	
3451~4350	24.00	6.50	3.75	See B.3.4*	
4351~5450	25.00	6.75	4.00	See B.3.4*	
5451~6800	26.00	7.00	4.00	See B.3.4*	
6801~8500	27.00	7.25	4.25	See B.3.4*	
8501~10700	28.00	7.50	4.50	See B.3.4*	
> 10,700	Follow progression above	Follow progression above	Follow progression above	See B.3.4*	

* refers to Annex B, paragraph B.3.4 of ISO/IEC 27006

10.2 The audit time chart above provides the framework that shall be used for audit planning by identifying a starting point based on the total number of persons doing work under the organisation's control for all shifts within the scope of the certification. Where a client organisation is both a PII Controller and a PII Processor, then the additional times shall be added before factors for adjusting audit time are considered.

10.3 It is expected that the time calculated for planning and report writing combined should not typically reduce the total on-site "audit time" to less than 70 % of the time calculated in accordance with ISO/IEC 27006, Annex B.3.3 and B.3.4. Where additional time is required for planning and/or report writing, this shall not be justification for reducing on-site audit time. Auditor travel time is not included in this calculation and is additional to the audit time referenced in the chart.

10.4 The number of total onsite auditor days – as calculated for the scope following the procedure stated in ISO/IEC 27006, Annex B.3.3 – shall be distributed amongst the different sites based on the relevance of the site for the management system and the risks identified. The justification for the distribution shall be recorded by the certification body.

10.5 The total time expended on initial assessment and surveillance is the total sum of the time spent at each site plus the central office and shall never be less than that which would have been calculated for the size and complexity of the operation if all the work had been undertaken at a single site (i.e. with all the employees of the company in the same site).

11. Certification Documents

11.1 The certification document(s) shall identify the scope of certification with respect to the type of activities, products and services as applicable at each site without being misleading or ambiguous.

11.2 Certification documents shall be signed by an officer who has been assigned such responsibility. The version of the Statement of Applicability shall be included in the certification documents.

11.3 The certification document(s) shall identify the management system standards in the form "ISO/IEC 27001:2013 as extended by ISO/IEC 27701:2019". The certificate shall not be misleading or ambiguous (e.g. the formatting shall not give prominence to the extension standard, ISO/IEC 27701, over the primary management system standard, ISO/IEC 27001, on which it is based);

11.4 Certification bodies shall ensure that the scope of certification reflects the protection of privacy (of PII principals as potentially affected by the processing of PII) *in addition to* information security within

the same overall scope of certification (i.e. the scope for privacy information management shall not be separate to the scope of the information security management system it is based on).

11.5 It is recognised that non-accredited certificates may have been issued whilst a certification body was working towards accreditation for ISO/IEC 27701. As a result of International Accreditation Forum (IAF) Resolution 2015-14 and in accordance with UKAS Publication TPS 65, paragraph 2.5 (regarding the issue of non-accredited management systems certificates in scopes for which a certification body is accredited) the certification body will have 30 days (from the date of grant of accreditation for ISO/IEC 27701) to take appropriate action to transfer previously issued non-accredited certificates to accredited ones. These actions may require the certification body to carry out a review and additional validation activities of each certificate before confirming its accredited status. Records of these reviews, including the supporting rationale for transferring to an accredited certificate, shall be retained for review during subsequent assessment activities.

11.6 In accordance with International Accreditation Forum (IAF) Resolution 2016-17, in order for a management system certification document to be considered accredited, it shall display the accreditation symbol, and/or, reference the accreditation status of the Certification Body including the identification of UKAS as the Accreditation Body.

12. Decisions on Certification

12.1 The group or individual that takes the decision on granting, refusing, maintaining, renewing, suspending, restoring, or withdrawing certification, or on expanding or reducing the scope of certification, shall understand the applicable standard and certification requirements, including those defined in ISO/IEC 27701, and shall have demonstrated competence to evaluate the outcomes of the audit processes including related recommendations of the audit team.

12.2 The certification body shall retain authority and responsibility for its decisions relating to certification including the grant, maintenance, renewing, extension, reduction and withdrawal of certification.

13. References

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

1. ISO/IEC 17021-1 *Conformity assessment - Requirements for bodies providing audit and certification of management systems Part 1: Requirements*

2. ISO/IEC 27006 *Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems*

3. ISO/IEC 27701 *Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines*

4. ISO/IEC 27000 *Information technology - Security techniques - Information security management systems - Overview and vocabulary*

5. ISO/IEC 29100:2011 as amended by ISO/IEC amendment A1:2018 *Information technology - Security techniques - Privacy framework*

6. UKAS publication GEN 1 *General Principles for the Assessment of Conformity Assessment Bodies by the United Kingdom Accreditation Service*

7. TPS 65 *UKAS Policy on Issuance of Accredited and Nonaccredited Certificates by Accredited Certification Bodies*