

|  |
| --- |
| **TRANSITION REQUIREMENTS** |

**Transition to ISO/IEC 27006-1:2024**

1. **Introduction and Scope**

The standard ISO/IEC 27006-1:2024 - *Requirements for bodies providing audit and certification of information security management systems — Part 1: General* was published on 01 March 2024. This edition of ISO/IEC 27006-1:2024 replaces ISO/IEC 27006:2015/AMD1:2020.

A transition period of 2 years has been agreed from the date of publication for accredited bodies to review the requirements and bring their operations and processes in line with the requirements of the new standard. As a consequence, UKAS will require all of its accredited bodies operating under this standard to have demonstrated conformity and transitioned to the new standard by 31 July 2025.

1. **Objective**

This document is aimed at providing all UKAS accredited bodies with details of the transition processes which will be implemented by UKAS and the information they will need to supply to assist this process.

1. **UKAS requirements for accredited bodies for the transition to ISO/IEC 27006-1:2024**
2. Accredited certification bodieswho are currently accredited to ISO/IEC 27006:2015/AMD1:2020 are advised to review the new standard, conduct a gap analysis and establish a transition plan to incorporate the required changes (where applicable) into their management system. Certification bodies are required to document their gap analysis and transition plan, submitting a copy to UKAS by 30 April 2024 to the following email address; applications@ukas.com. This information should be submitted using the attached template (Annex 1) and must be accompanied by any relevant supporting documentation (clearly indexed using the table in Annex 1).
3. The UKAS transition process will consist of the following assessment stages:
* Review of the Gap Analysis, Plan and related documentation;
* Head Office assessment (if required).

**NOTE**: Additional time and effort may be required during the transition process, for example for the review of the Gap Analysis. Any additional time and effort will be quoted in advance of the activity taking place.

1. Mandatory Improvement Actions (IARs) which are raised against the new standard will need to be cleared prior to the grant of accreditation. Where verification of the effectiveness of the corrective actions is deemed necessary further on site activity may be required.
2. If the accredited body fails to demonstrate conformity to ISO/IEC 27006-1:2024 and/or clear those improvements actions raised before the transition deadline, the body shall be suspended for a maximum of 6 months. If the body fails to address those actions required to complete the transition process within this timeframe, this would result in the withdrawal of accreditation for Information Security Management Systems certification.
3. **New Applications/Extensions to Scope:**
4. All new applications/extensions to scope received after 01 May 2024 shall be assessed against ISO/IEC 27006-1:2024
5. For existing applicants, assessments which are scheduled to take place after 01 May 2024 shall be against ISO/IEC 27006-1:2024
6. **Validity of ISO/IEC 27006:2015/AMD1:2020**

ISO/IEC 27006:2015/AMD1:2020 will cease to be valid on 31 March 2026.

1. **Projected Timetable**

**The following timetable is based on our current knowledge and the publication of ISO/IEC 27006-1:2024 on 01 March 2024. Please note that should dates or actions change UKAS will provide updates via the Technical Bulletins posted on the UKAS website** [www.ukas.com](http://www.ukas.com)

|  |  |
| --- | --- |
| **Date**  | **Milestone/Activity** |
| **01 March 2024** | **Publication of ISO/IEC 27006-1:2024** |
| **01 May 2024** | **UKAS ready to assess to ISO/IEC 27006-1:2024** |
| **31 July 2025** | **All UKAS transitions of CB’s completed** |

**Annex 1**

**Gap Analysis and Transition Plan**

|  |  |
| --- | --- |
| **Name of Organisation** | Click here to enter text |
| **Accreditation Number** | Click here to enter text |
| **Date of Submission** | Select a date from the calendar |

**GAP ANALYSIS**

| **CLAUSE** | **ISO/IEC 27006:2015/AMD1:2020** | **CLAUSE** | **ISO/IEC 27006-1:2024** | **CABs DETERMINATION OF EXTENT OF CHANGE** | **DETAILS OF CHANGES WITHIN YOUR MANAGEMENT SYSTEM WHICH HAVE/WILL BE TAKEN TO ADDRESS CHANGES** | **UKAS COMMENTS REGARDING INFORMATION SUPPLIED INCLUDING REFERENCE TO ANY IARS RAISED** |
| --- | --- | --- | --- | --- | --- | --- |
|  | Foreward  |  | Foreward  |  |  |  |
|  | Introduction  |  | Introduction  |  |  |  |
| 1. | Scope  | 1. | Scope  |  |  |  |
| 2. | Normative references | 2. | Normative references  |  |  |  |
| 3. | Terms & Definitions | 3. | Terms & Definitions |  |  |  |
| 4.  | Principles | 4.  | Principles |  |  |  |
| 5.  | General requirements | 5.  | General requirements |  |  |  |
| 5.1 | Legal and contractual matters | 5.1 | Legal and contractual matters |  |  |  |
| 5.2 | Management of impartiality | 5.2 | Management of impartiality |  |  |  |
|  |  | 5.2.1 | General |  |  |  |
| 5.2.1 | IS 5.2 Conflicts of interest | 5.2.2 | Conflicts of interest |  |  |  |
| 5.3 | Liability and financing | 5.3 | Liability and financing |  |  |  |
| 6. | Structural requirements | 6. | Structural requirements |  |  |  |
| 7. | Resource requirements | 7. | Resource requirements |  |  |  |
| 7.1 | Competence of personnel | 7.1 | Competence of personnel |  |  |  |
| 7.1.1 | IS 7.1.1 General considerations | 7.1.1 | General  |  |  |  |
| 7.1.1.1 | Generic competence requirements | 7.1.2 | Generic competence requirements |  |  |  |
| 7.1.2 | IS 7.1.2 Determination of Competence Criteria | 7.1.3 | Determination of Competence Criteria |  |  |  |
| 7.1.2.1 | Competence requirements for ISMS auditing | 7.1.3.1 | Competence requirements for ISMS auditing |  |  |  |
| 7.1.2.1.1 | General requirements | 7.1.3.1.1 | General requirements |  |  |  |
| 7.1.2.1.2 | Information security management terminology, principles, practices and techniques | 7.1.3.1.2 | Information security management terminology, principles, practices and techniques |  |  |  |
| 7.1.2.1.3 | Information security management system standards and normative documents | 7.1.3.1.3 | Information security management system standards and normative documents |  |  |  |
| 7.1.2.1.4 | Business management practices | 7.1.3.1.4 | Business management practices |  |  |  |
| 7.1.2.1.5 | Client business sector | 7.1.3.1.5 | Client business sector |  |  |  |
| 7.1.2.1.6 | Client products, processes and organization | 7.1.3.1.6 | Client products, processes and organization |  |  |  |
| 7.1.2.2 | Competence requirements for leading the ISMS audit team | 7.2.2.4 | *See below* |  |  |  |
| 7.1.2.3 | Competence requirements for conducting the application review | 7.1.3.2 | Competence requirements for conducting the application review |  |  |  |
| 7.1.2.3.1 | Information security management system standards and normative documents |  |  |  |  |  |
| 7.1.2.3.2 | Client business sector | 7.1.3.2.1 | Client business sector |  |  |  |
| 7.1.2.3.3 | Client products, processes and organization | 7.1.3.2.2 | Client products, processes and organization |  |  |  |
| 7.1.2.4 | Competence requirements for reviewing audit reports and making certification decisions | 7.1.3.3 | Competence requirements for reviewing audit reports and making certification decisions |  |  |  |
| 7.1.2.4.1 | General | 7.1.3.3.1 | General |  |  |  |
| 7.1.2.4.2 | Information security management terminology, principles, practices and techniques | 7.1.3.3.2 | Information security management terminology, principles, practices and techniques |  |  |  |
| 7.1.2.4.3 | Information security management system standards and normative documents |  |  |  |  |  |
| 7.1.2.4.4 | Client business sector | 7.1.3.3.3 | Client business sector |  |  |  |
| 7.1.2.4.5 | Client products, processes and organization | 7.1.3.3.4 | Client products, processes and organization |  |  |  |
| 7.2 | Personnel involved in the certification activities | 7.2 | Personnel involved in the certification activities |  |  |  |
|  |  | 7.2.1 | General |  |  |  |
| 7.2.1 | IS 7.2 Demonstration of auditor knowledge and experience | 7.2.2 | Demonstration of auditor knowledge and experience |  |  |  |
|  |  | 7.2.2.1 | General considerations |  |  |  |
| 7.2.1.1 | Selecting auditors | 7.2.2.2 | Selecting auditors |  |  |  |
|  |  | 7.2.2.3 | Selecting technical experts |  |  |  |
| 7.2.1.2 | Selecting auditors for leading the team | 7.2.2.4 | Selecting auditors for leading the team |  |  |  |
| 7.3 | Use of individual external auditors and external technical experts | 7.3 | Use of individual external auditors and external technical experts |  |  |  |
| 7.3.1 | IS 7.3 Using external auditors or external technical experts as part of the audit team |  |  |  |  |  |
| 7.4 | Personnel records | 7.4 | Personnel records |  |  |  |
| 7.5 | Outsourcing | 7.5 | Outsourcing |  |  |  |
| 8 | Information requirements | 8 | Information requirements |  |  |  |
| 8.1 | Public information | 8.1 | Public information |  |  |  |
| 8.2 | Certification documents | 8.2 | Certification documents |  |  |  |
|  |  | 8.2.1 | General |  |  |  |
| 8.2.1 | IS 8.2 ISMS Certification documents | 8.2.2 | ISMS Certification documents |  |  |  |
|  |  | 8.2.3 | Reference of other standards in the ISMS certification documents |  |  |  |
| 8.3 | Reference to certification and use of marks | 8.3 | Reference to certification and use of marks |  |  |  |
| 8.4 | Confidentiality | 8.4 | Confidentiality |  |  |  |
|  |  | 8.4.1 | General |  |  |  |
| 8.4.1 | IS 8.4 Access to organizational records | 8.4.2 | Access to organizational records |  |  |  |
| 8.5 | Information exchange between a certification body and its clients | 8.5 | Information exchange between a certification body and its clients |  |  |  |
| 9 | Process requirements | 9 | Process requirements |  |  |  |
| 9.1 | Pre-certification activities | 9.1 | Pre-certification activities |  |  |  |
| 9.1.1 | Application | 9.1.1 | Application |  |  |  |
|  |  | 9.1.1.1 | General |  |  |  |
| 9.1.1.1 | IS 9.1.1 Application readiness |  |  |  |  |  |
| 9.1.2 | Application review |  |  |  |  |  |
|  |  | 9.1.2 | Application review |  |  |  |
| 9.1.3 | Audit programme | 9.1.3 | Audit programme |  |  |  |
|  |  | 9.1.3.1 | General |  |  |  |
| 9.1.3.1 | IS 9.1.3 General | 9.1.3.2 | General considerations |  |  |  |
| 9.1.3.2 | IS 9.1.3 Audit Methodology | 9.1.1.2 | Considerations for Certification Procedures |  |  |  |
|  |  | 9.1.3.3 | Deployment of remote audit |  |  |  |
| 9.1.3.3 | IS 9.1.3 General preparations for the initial audit | 9.1.3.4 | General preparations for the initial audit |  |  |  |
| 9.1.3.4 | IS 9.1.3 Review periods | 9.1.3.5 | Review periods |  |  |  |
| 9.1.3.5 | IS 9.1.3 Scope of certification | 9.1.3.6 | Scope of ISMS certification |  |  |  |
| 9.1.3.6 | IS 9.1.3 Certification audit criteria |  |  |  |  |  |
| 9.1.4 | Determining audit time | 9.1.4 | Determining audit time |  |  |  |
|  |  | 9.1.4.1 | General |  |  |  |
| 9.1.4.1 | IS 9.1.4 Audit time | 9.1.4.2 | Audit time |  |  |  |
| 9.1.5 | Multi-site sampling | 9.1.5 | Multi-site sampling |  |  |  |
|  |  | 9.1.5.1 | General |  |  |  |
| 9.1.5.1 | IS 9.1.5 Multiple sites | 9.1.5.2 | Multiple sites |  |  |  |
| 9.1.6 | Multiple management systems | 9.1.6 | Multiple management systems |  |  |  |
|  |  | 9.1.6.1 | General |  |  |  |
| 9.1.6.1 | IS 9.1.6 Integration of ISMS documentation with that for other management systems | 9.1.6.2 | Integration of ISMS and other management system documentation |  |  |  |
| 9.1.6.2 | IS 9.1.6 Combining management system audits | 9.1.6.3 | Combining management system audits |  |  |  |
| 9.2 | Planning audits | 9.2 | Planning audits |  |  |  |
| 9.2.1 | Determining audit objectives, scope and criteria | 9.2.1 | Determining audit objectives, scope and criteria |  |  |  |
|  |  | 9.2.1.1 | General |  |  |  |
| 9.2.1.1 | IS 9.2.1 Audit objectives | 9.2.1.2 | Audit objectives |  |  |  |
|  |  | 9.2.1.3 | Audit criteria |  |  |  |
| 9.2.2 | Audit team selection and assignments | 9.2.2 | Audit team selection and assignments |  |  |  |
| 9.2.2.1 | IS 9.2.2 Audit team | 9.2.2.1 | General |  |  |  |
| 9.2.2.2 | IS 9.2.2 Audit team competence |  |  |  |  |  |
| 9.2.3 | Audit plan | 9.2.3 | Audit plan |  |  |  |
|  |  | 9.2.3.1 | General |  |  |  |
| 9.2.3.1 | IS 9.2.3 General | 9.2.3.2 | General considerations |  |  |  |
| 9.2.3.2 | IS 9.2.3 Network-assisted audit techniques | 9.2.3.3 | Remote audit techniques |  |  |  |
| 9.2.3.3 | IS 9.2.3 Timing of audit |  |  |  |  |  |
| 9.3 | Initial certification | 9.3 | Initial certification |  |  |  |
|  |  | 9.3.1 | General |  |  |  |
| 9.3.1 | IS 9.3.1 Initial certification audit | 9.3.2 | Initial certification audit |  |  |  |
| 9.3.1.1 | IS 9.3.1.1 Stage 1 | 9.3.2.1 | Stage 1 |  |  |  |
| 9.3.1.2 | IS 9.3.1.2 Stage 2 | 9.3.2.2 | Stage 2 |  |  |  |
| 9.4 | Conducting audits | 9.4 | Conducting audits |  |  |  |
| 9.4.1 | IS 9.4 General | 9.4.1 | General |  |  |  |
| 9.4.2 | IS 9.4 Specific elements of the ISMS audit | 9.4.2 | Specific elements of the ISMS audit |  |  |  |
| 9.4.3 | IS 9.4 Audit report | 9.4.3 | Audit report |  |  |  |
| 9.5 | Certification decision | 9.5 | Certification decision |  |  |  |
|  |  | 9.5.1 | General |  |  |  |
| 9.5.1 | IS 9.5 Certification decision | 9.5.2 | Certification decision |  |  |  |
| 9.6 | Maintaining certification | 9.6 | Maintaining certification |  |  |  |
| 9.6.1 | General | 9.6.1 | General |  |  |  |
| 9.6.2 | Surveillance activities | 9.6.2 | Surveillance activities |  |  |  |
| 9.6.2.1 | IS 9.6.2 Surveillance activities |  |  |  |  |  |
| 9.6.3 | Re-certification | 9.6.3 | Re-certification |  |  |  |
| 9.6.3.1 | IS 9.6.3 Re-certification audits | 9.6.3.1 | General |  |  |  |
|  |  | 9.6.3.2 | Re-certification audits |  |  |  |
| 9.6.4 | Special audits | 9.6.4 | Special audits |  |  |  |
| 9.6.4.1 | IS 9.6.4 Special cases |  |  |  |  |  |
| 9.6.5 | Suspending, withdrawing or reducing the scope of certification |  |  |  |  |  |
| 9.7 | Appeals | 9.7 | Appeals |  |  |  |
| 9.8 | Complaints | 9.8  | Complaints |  |  |  |
|  |  | 9.8.1 | General |  |  |  |
| 9.8.1 | IS 9.8 Complaints | 9.8.2 | Complaints |  |  |  |
| 9.9 | Client records | 9.9 | Client records |  |  |  |
| 10 | Management system requirements for certification bodies | 10 | Management system requirements for certification bodies |  |  |  |
| 10.1 | Options | 10.1 | Options |  |  |  |
| 10.1.1 | IS 10.1 ISMS implementation | 10.1.1 | IS 10.1 ISMS implementation |  |  |  |
| 10.2 | Option A: General management system requirements | 10.2 | Option A: General management system requirements |  |  |  |
| 10.3 | Option B: Management system requirements in accordance with ISO 9001 | 10.3 | Option B: Management system requirements in accordance with ISO 9001 |  |  |  |
| Annex A(informative) | Knowledge and skills for ISMS auditing and certification | Annex A(normative) | Knowledge and skills for ISMS auditing and certification |  |  |  |
| A.1 | Overview | A.1 | Overview |  |  |  |
|  |  | Annex B (informative) | Further competence considerations |  |  |  |
| A.2 | General competence considerations | B.1 | General competence considerations |  |  |  |
| A.3 | Specific knowledge and experience considerations | B.2 | Specific knowledge and experience considerations |  |  |  |
| A.3.1 | Typical knowledge related to ISMS | B.2.1 | Typical knowledge related to ISMS |  |  |  |
| Annex B (normative) | Audit time | Annex C(normative) | Audit time |  |  |  |
| B.1 | Introduction | C.1 | General |  |  |  |
| B.2 | Concepts | C.2 | Concepts |  |  |  |
| B.2.1 | Number of persons doing work under the organization’s control | C.2.1 | Number of persons doing work under the organization’s control |  |  |  |
| B.2.2 | Auditor day | C.2.2 | Auditor day |  |  |  |
| B.2.3 | Temporary site | C.2.3 | Temporary site |  |  |  |
| B.3 | Procedure for determining audit time for initial audit | C.3 | Procedure for determining audit time for initial audit |  |  |  |
| B.3.1 | General | C.3.1 | General |  |  |  |
| B.3.2 | Remote audit | C.3.2 | Remote methods for conducting audit |  |  |  |
| B.3.3 | Audit time calculation | C.3.3 | Audit time calculation |  |  |  |
|  |  | C.3.4 | Determination of initial number of persons |  |  |  |
| B.3.4 | Factors for adjustment of audit time | C.3.5 | Factors for adjustment of audit time |  |  |  |
| B.3.5 | Limitation of deviation of audit time | C.3.6 | Limitation of deviation of audit time |  |  |  |
| B.3.6 | On-site audit time | C.3.7 | On-site audit time |  |  |  |
| B.4 | Audit time for surveillance audit | C.4 | Audit time for surveillance audit |  |  |  |
| B.5 | Audit time for re-certification audit | C.5 | Audit time for re-certification audit |  |  |  |
| B.6 | Audit time of multi-site | C.6 | Audit time of multi-site |  |  |  |
|  |  | C.7 | Audit time for scope extensions |  |  |  |
| Annex C (informative) | Methods for audit time calculations | Annex D (informative) | Methods for audit time calculations |  |  |  |
| C.1 | General | D.1 | General |  |  |  |
| C.2 | Classification of factors for calculating audit time | D.2 | Classification of factors for calculating audit time |  |  |  |
| C.3 | Example for audit time calculation | D.3 | Example for audit time calculation |  |  |  |
| Annex D (information) | Guidance for review of implemented ISO/IEC 27001:2013, Annex A controls | Annex E(informative) | Guidance for review of implemented ISO/IEC 27001:2022, Annex A controls |  |  |  |
| D.1 | Purpose |  |  |  |  |  |
| D.1.1 | Audit evidence |  |  |  |  |  |
| D.2 | How to use Table D.1 | E.2 | How to use Table E.1 |  |  |  |
| D.2.1 | General | E.2.1 | General |  |  |  |
| D.2.2 | Columns “Organizational control” and “Technical control” |  |  |  |  |  |
| D.2.3 | Column “System testing” | E.2.2 | Column “System testing” |  |  |  |
| D.2.4 | Column “Visual inspection” | E.2.3 | Column “Visual inspection” |  |  |  |
| D.2.5 | Column “Audit review guidance” | E.2.4 | Possible evidence of design and implementation of controls |  |  |  |
|  | Bibliography |  | Bibliography |  |  |  |

**TRANSITION PLAN**

\**please detail in the table below the actions taken, or to be taken (with timescales) to complete the transition to this new standard/scheme within your organisation*

|  |  |  |
| --- | --- | --- |
| **ACTION** | **TIMESCALE** | **OWNER** |
| Example:, develop training plan, update documentation, complete internal audit, notify customers, complete assessments  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**DOCUMENTATION**

**\****please index in the table below the documentation supplied in support of your transition with this Gap Analysis and Transition Plan.*

|  |  |  |
| --- | --- | --- |
| **DOCUMENT REFERENCE** | **DOCUMENT NAME** | **VERSION NUMBER**  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |