UNITED ACCREDITATION FOUNDATION

Document Name	**ACCREDITATION REQUIREMENTS FOR CERTIFICATION OF INFORMATION SECURITY MANAGEMENT SYSTEMS (ISMS)**
Document Number	**UAF-CAB-ISMS**
Applicable For	**All Certification Bodies applying for ISMS**
Revision Number	**V00**
Revision Date	**NOV-15-2024**
Effective Date	**NOV-15-2024**

Contents

1. ACCREDITATION REQUIREMENTS

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

2. ADDITIONAL DOCUMENTS

ISO/IEC, IAF and other applicable requirements applicable for accreditation of ISO 27001 certification:

- ISO/IEC 27006, Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems
- IAF MD 1: IAF Mandatory Document for the Audit and Certification of a Management System Operated by a Multi-Site Organization
- IAF MD 2: IAF Mandatory Document for the Transfer of Accredited Certification of Management Systems.
- IAF MD 4: IAF Mandatory Document for the Use of Information and Communication Technology (ICT) for Auditing/Assessment Purposes
- IAF MD 5: Determination of Audit Time of Quality, Environmental, and Occupational Health & Safety Management Systems.
- IAF MD 11: IAF Mandatory Document for Application of ISO/IEC 17021 for Audits of Integrated Management Systems (IMS)
- IAF MD 23:Control of Entities Operating on Behalf of Accredited Management Systems Certification Bodies
- IAF MD 28: IAF Mandatory Document for the Upload and Maintenance of Data on IAF Database (Application date October 26, 2024)

3. UAF DOCUMENTS APPLICABLE FOR ACCREDITATION OF ISO 27001 CERTIFICATION

- UAF-GEN-CAB-01-General Accreditation requirements
- UAF-GEN-CAB-02-Conditions for the use of UAF Symbol
- UAF-PL:2014-01: Policy on providing conformity assessment in countries without the country's relevant authority's approval.
- UAF F-31A-Annexure A- Guidance for the addition of countries, locations and critical Locations.
- UAF-PL:2016-06: UAF Policy for the Collection of Data to Provide Indicators of Management System Certification Bodies' Performance as per IAF MD 15:2014.
- UAF-PL:2018-04: UAF Policy on handling misconduct & unethical practices in the certification process
- UAF-PL:2019-07-01: UAF Policy on accreditation scopes & witnessing activities for accreditation of management system CBs
- UAF-PL:2019-07-02: UAF Policy regarding general administration
- UAF-PL:2020-03-02: UAF Policy for handling extraordinary events or circumstances affecting UAF Accredited CABs on their certified clients/persons.

- UAF-PL:2020-03-03: UAF Policy on Remote Assessment
- UAF-PL:2023-09-01: UAF Policy for CAB operations in Sanctioned Countries
- UAF-PL:2024-02-01: UAF policy regarding the consideration of climate change within the organizational context of the management system

4. CERTIFICATION DOCUMENTS

Certification bodies (CAB) certify against ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements.

5. SCOPE OF ACCREDITATION

Certification of Information Security Management Systems (ISMS) Accreditation provided in accordance with ISO/IEC 27006.

6. REQUIREMENTS

6.1 Management of impartiality

The requirements from ISO/IEC 17021-1:2015, Clause 5.2 apply and in addition, the ISMSspecific requirements and guidance apply as detailed in ISO/IEC 27006.

7. RESOURCE REQUIREMENTS

7.1 Competence of management and personnel

The requirements from ISO/IEC 17021-1:2015, Clause 7.1 apply and in addition, the ISMSspecific requirements and guidance apply as detailed in ISO/IEC 27006.

7.2 Personnel involved in the certification activities

The requirements from ISO/IEC 17021-1:2015, Clause 7.2 apply and in addition, the ISMSspecific requirements and guidance apply as detailed in ISO/IEC 27006.

7.3 Use of individual external auditors and external technical experts

The requirements from ISO/IEC 17021-1:2015, Clause 7.3 apply in addition, the ISMSspecific requirements and guidance apply as detailed in ISO/IEC 27006.

8. INFORMATION REQUIREMENTS

8.1 Publicly accessible information

The requirements from ISO/IEC 17021-1:2015, Clause 8.1 apply in addition, the ISMSspecific requirements and guidance apply as detailed in ISO/IEC 27006.

8.2 **Certification documents**

The requirements from ISO/IEC 17021-1:2015, Clause 8.2 apply in addition, the ISMSspecific requirements and guidance apply as detailed in ISO/IEC 27006.

8.3 **Reference to certification and use of marks**

The requirements from ISO/IEC 17021-1:2015, Clause 8.3 apply in addition, the ISMSspecific requirements and guidance apply as detailed in ISO/IEC 27006.

8.4 **Confidentiality**

The requirements from ISO/IEC 17021-1:2015, Clause 8.4 apply. In addition, the ISMSspecific requirements and guidance apply as detailed in ISO/IEC 27006.

9. PROCESS REQUIREMENTS

9.1 **General requirements**

In addition, the ISMS-specific requirements and guidance apply as detailed in ISO/IEC 27006.

9.2 **Initial Assessments**

The assessment extent and content depend on the requested scope of accreditation, the other activities for which the body is accredited or requests accreditation and the performance of the body at previous assessments.
The Assessment consists of following activities:

- Document Review
- Office assessment
- Witness Assessments
- Scope Verifications during extraordinary circumstances.

In addition, the ISMS-specific requirements and guidance as stated in clause 9.3 of ISO/IEC 27006 apply.

10. SURVEILLANCE AND REASSESSMENTS

10.1 In addition, the ISMS-specific requirements and guidance as stated in ISO/IEC 27006 for Surveillance and for recertification shall apply.

10.2 The implementation of the ISO 27001 certification system will be verified during each surveillance assessment being conducted by UAF. The files reviewed during the subsequent surveillances and the reassessment in a four years' period (accreditation cycle) shall be as per the requirements of IAF MD 17 and ISO/IEC 27006. The number of files to be reviewed for each assessment is calculated based on the number of certificates issued since the last assessment. This is approximately one-tenth of the square root of the number of certificates,

with a maximum of six files and a minimum of one file. The number of files to be reviewed may increase depending on risk-based parameters detailed in the assessment program.

10.3 The application of applicable IAF MD documents shall be verified during each assessment as detailed in assessment plan.

10.4 For each accreditation cycle (surveillances and reassessment), the number of witnesses will be determined as per the assessment program in line with requirements of IAF MD 17 and UAF witness policy. The number of witnesses may vary as per the outcome of client files reviews in line with UAF witness policy document and as per applicable mandatory documents such as IAF MD17/accreditation standard requirements.

10.5 In the application of the above guidelines, it shall be considered whether witness assessments may serve for multiple schemes (e.g., by witnessing combined audits) and how may witness assessments are performed in other schemes.

11. COMPLAINTS

In addition, the ISMS-specific requirements and guidance as stated in clause 9.8 of ISO/IEC 27006:2015 apply.

12. GENERAL REMARKS ON WITNESSING

Generally, two weeks before the witnessing, the CB shall provide the UAF team with following:

- The records of the CB's contract review for the selected organization (including qualification records for the auditors used).
- The output (records/procedures) of the organization to be audited related to their determination of significant energy impacts of the organisation and the energy efficiency plan for the upcoming period
- A copy of the ISO 27001 certificate issued by the CB, in case a surveillance or recertification audit is being witnessed.
- For CABs already accredited by IAF Full Members AB, Earlier Witness reports may be accepted.
- The report of the CB's pre-assessment or stage 1 assessment of the organization's MS (or other latest report) and an audit plan.

Besides the considerations mentioned above for selection of audits to be witnessed, UAF will also consider the following:

- UAF will normally not witness the same auditors that have been witnessed in the same scheme before.
- UAF will normally not witness an audit at the same organization. • UAF will review of the audit report as part of the witness audit.

To be able to select the audits to be witnessed, the CB shall, on request of UAF, provide a planning for the audits to be conducted in a certain period. The information on these audits shall include as a minimum:

- Type of audit (initial, recertification or surveillance).
- Name and address of the auditee.
- Audit standard(s).
- Scope of certification.
- Name(s) of auditors(s) and expert(s).
- Date(s) of the audit.