Certification Regulation for Information Security MS Remote Audits

Standard or Certification scheme:	**ISO/IEC 27001:2022** **ISO 27701:2019**	**Accreditation Standard:**	**ISO 17021-1:2015**

Certification Cycle:

The certificate is valid for three years. To maintain the validity of the certificate, annual surveillance audits shall be carried out. Before the expiration date of the certificate, a recertification audit is conducted in order to renew the validity of the certificate for the next three year cycle.

Audit planning and time table. Surveillance audit process has to be completed annually, with due date the date of the certification decision after the Initial Certification audit. Correspondingly the re-certification audit process has to be completed within the same time frame. Example:

Certification Decision	**1st Surveillance audit**	**2nd Surveillance**	**Re-certification audit**
15/7/2023	*15/7/2024*	*15/7/2025*	*15/7/2025*

In case of exceeding time limits certificate is suspended for six months and after this period is finally withdrawn.

Audit Conduction Procedure ISO/IEC 27001:

The certification procedure is conducted in two stages:

Stage 1: At least the following information shall be provided by the client during Stage 1 of the certification audit:

- ✔ General information concerning the ISMS and the activities it covers.
- ✔ A copy of the required ISMS documentation specified in ISO/IEC 27001 and where required, other association documentation.

TÜV Austria has the obligation to assess the above mentioned documentation in order to certify the followings:

- ✔ ISMS documentation covering the documentation required in ISO/IEC 27001.
- ✔ Sufficient understanding of the design of the ISMS in the context of the client's organization, risk assessment and treatment (including the controls determined), information security policy and objectives and, in particular, of the client's preparedness for the audit.

Stage 2: The objectives of Stage 2 are:

- ✔ TÜV Austria has the obligation to confirm that the client adheres to its own policies, objectives and procedures.

To do this, the audit shall focus on the client's:

- ✔ Top management leadership and commitment to the information security objectives.
- ✔ Assessment of information security related risks. The audit shall also ensure that the assessments produce consistent, valid and comparable results, if repeated.
- ✔ Determination of controls based on the information security risk assessment and risk treatment processes.
- ✔ Information security performance and the effectiveness of the ISMS, evaluating these against the information security objectives.
- ✔ Correspondence between the determined controls, the Statement of Applicability, the results of the information security risk assessment, the risk treatment process and the information security policy and objectives.

	✔ Implementation of controls, taking into account the external and internal context and related risks, and the organization's monitoring, measurement and analysis of information security processes and controls, to determine whether controls declared as being implemented are actually implemented and effective as a whole. ✔ Programmes, processes, procedures, records, internal audits and reviews of the ISMS effectiveness to ensure that these are traceable to top management decisions and the information security policy and objectives. **Surveillance – Recertification** The purpose of surveillance is to verify that the approved ISMS continues to be implemented, to consider the implications of changes to that system initiated as a result of changes in the client's operation and to confirm continued compliance with certification requirements. Surveillance audit programmes shall cover at least: ✔ The ISMS maintenance elements such as information security risk assessment and control maintenance, internal ISMS audit, management review and corrective action. ✔ Communications from external parties as required by the ISMS standard ISO/IEC 27001 and other documents required for certification. As a minimum, every surveillance by TÜV Austria shall review the following: ✔ The effectiveness of the ISMS with regard to achieving the objectives of the client's information security policy. ✔ The functioning of procedures for the periodic evaluation and review of compliance with relevant information security legislation and regulations. ✔ Changes to the controls determined, and resulting changes to the SoA. ✔ Implementation and effectiveness of controls according to the audit programme. The rest of the elements are Audited during the two surveillance audits, in such a way that every element of the system is audited after the two surveillance audits at least once. During the onsite recertification audit the following topics are evaluated: ✔ Restoration of the observations and / or non-conformities of the previous audit ✔ All the topics mentioned at Stage 2 of the certification audit
Audit Conduction Procedure ISO/IEC 27701	Certification to ISO/IEC 27001 is obligatory in order to obtain certification for ISO/IEC27701. The scope of the ISO/IEC 27701 certification: ✔ Is within or identical to the scope of the ISO/IEC 27001 certification. ✔ Is included within boundaries of the activities of the client as defined in the scope of the PIMS. ✔ PII processing is included The audit programme for an ISO/IEC 27701 audit identifies the role of the client with regard to PII controllers and PII processors. The audit plan shall take the PIMS controls into account. The role of the client (PII controller, PII processor or both) is described in the audit report. The audit report provides the overview of the audit of the client's privacy impact assessment, or a reference to it. TÜV Austria considers the impact that a nonconformity found for the ISO/IEC 27701 requirements has an impact on the conformity with ISO/IEC 27001 and report accordingly. TÜV Austria will suspend, withdraw or reduce the scope of certification of ISO/IEC 27701 where its base ISO/IEC 27001 certification is suspended, withdrawn or its scope (which includes the scope of ISO/IEC 27701 certification) is reduced.

Audit Evaluation Criteria / Characterization of Non Conformities:	**1:** Full conformity	**3:** Minor Non-Conformity(-ies): reviewed and accepted the client's plan for correction and corrective action
	2: Observation, the effectiveness of the corrective action is evaluated during the next audit	**4:** Major Non-Conformity(-ies): Correction through submission of Documents or Re-audit
	OFI: Opportunities for Improvement: No further action is required by the client	
Time allowed to close Non Conformities:	Certification Audit: 2 months after the completion of stage 2. Surveillance Audit: 2 months after the date of the audit or no later than the due date of the certification decision. Recertification Audit: 2 months after the date of the audit or no later than the due date of the certification decision.	
Contractual Duration:	The duration of the service and the contractual obligation comes into force upon signature by both parties (TÜV AUSTRIA and Client Organization) and is valid for (3) three years of the relevant offer in cases of initial certification or re - certification. In case of Accredited Certification Transfer, the duration covers the validity period of the transferred certificate. In case of transition to a new version of the standard, the duration of contractual obligation is valid until the certification expiry date mentioned on the relative paragraph of the regulation.	