GUIDE

for

Conducting System Certifications in the Field of Information Security Management Systems acc. to ISO/IEC 27001
根据 ISO/IEC 27001 信息安全管理体系认证实施规则

(for internal use only 仅供内部使用)

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

Table of Contents 目录:

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

1. Introduction 引言

This guideline applies to all accredited conformity assessment procedures relating to the management system standard ISO/IEC 27001 until this guideline is declared to be invalid or replaced by a new version.本指南适用于与管理体系标准 ISO/IEC 27001 相关的所有经认可的合格评定程序，直至本指南被宣布无效或被新版本所取代。

The specifications of Quality Austria as well as the requirements stated in ISO/IEC 27006:2015 "Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems" and IAF Mandatory Document "Knowledge Requirements for Accreditation Body Personnel for Information Security Management Systems (ISO/IEC 27001)" (IAF MD 13:2023, Issue 2) will have to be followed for all system certifications in connection with this guideline. In order to maintain customer certification, these requirements will have to be met permanently.在依据本指南进行的所有体系认证中，都必须遵循 Quality Austria 的规范，以及 ISO/IEC 27006:2015《信息技术—安全技术—提供信息安全管理体系审核和认证的机构的要求》和国际认可论坛（IAF）强制性文件《信息安全管理体系（ISO/IEC 27001）认可机构人员的知识要求》（IAF MD 13:2023，第 2 版）中规定的要求。为了维持客户的认证资格，必须始终满足这些要求。

For other specific certifications in the field of information security (e.g. Tisax, etc.), system evaluations and verifications will be conducted in cooperation with CIS - Certification & Information Security Services GmbH.对于信息安全领域的其他特定认证（如可信信息安全评估交换标准（Tisax）等），将与 CIS 认证与信息安全服务 GmbH 合作开展体系评估和验证工作。

2. qualityaustria policy for certification qualityaustria 认证政策

Upon organization's request, Quality Austria will conduct audits and other conformity assessment activities required for information security management systems certification for ISO/IEC 27001.应组织的要求，Quality Austria 将开展 ISO/IEC 27001 信息安全管理体系认证所需的审核及其他合格评定活动。

Quality Austria supports the use of integrated management systems. Among other things, use of integrated management systems serves to utilize synergies of information security management systems that may already be applied and other fields like quality management, environmental management, occupational health and safety management etc. Accordingly, Quality Austria offers its services wherever possible, as combined audits. Quality Austria 支持综合管理体系的运用。综合管理体系的运用，除其他方面外，有助于利用可能已应用的信息安全管理体系与质量管理、环境管理、职业健康与安全管理等其他领域之间的协同效应。因此，Quality Austria 尽可能以联合审核的形式提供服务。

Quality Austria employs personnel adequately qualified for its activities and ensures maintenance of the high technical competence by means of training and further training. Quality Austria 所聘用的人员具备与其业务活动相匹配的充足资质，并通过培训和持续培训来确保维持较高的技术能力水平。

Quality Austria promotes the large acceptability of its Certificates among users and its international certification partners. Quality Austria 致力于提高其证书在用户和国际认证合作伙伴中的广泛认可度。

For conducting certification, impartiality of Quality Austria and its auditors towards the customers must be guaranteed. Among other things, Quality Austria and its auditors must not be involved in designing, implementing or maintaining the information security management system which they review in an audit.在开展认证工作时，必须保证 Quality Austria 及其审核员对客户的公正性。其中，Quality Austria 及其审核员不得参与他们在审核中所审查的信息安全管理体系的设计、实施或维护工作。

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

3. Registration and making the offer 登记和报价

3.1 Defining the Time needed for audits acc. to ISO/IEC 27001

根据 ISO/IEC 27001 定义审核所需的时间

General Note: The audit time and how it is applied **is defined in ISO/IEC 27006:2015** and reported here in this guidance in this section. It is the responsibility of the auditor to plan the correct audit time in line with this guidance. Any proposed audit time, which is sent through a WIS order and corresponds to the table below must be verified by the auditor, also regarding factors that increase or reduce the audit time**. A justification of the adapted audit time** shall be sent to the Customer Service Center as evidence. The Customer Service Center (in case of complex orders in cooperation with the product expert) will give the final ok to the proposed audit time (no specific answer is needed if time is ok). A good method for this is to **use the IMS calculator** (see below) and send the filled excel (or a screen shot of the page) to the CSC.
一般说明：审核时间及其应用方式在 ISO/IEC 27006:2015 中有明确规定，并在本指南的本节中予以阐述。审核员有责任按照本指南规划合理的审核时间。通过 WIS 订单发送的、与下表相符的任何拟定审核时间，审核员都必须进行核实，同时要考虑到增加或减少审核时间的各项因素。经调整后的审核时间的说明应作为证明材料发送至客户服务中心。客户服务中心（对于复杂订单，将与产品专家合作）将对拟定的审核时间给出最终的批准意见（若时间合适，则无需给出具体答复）。一个较好的方法是使用综合管理体系（IMS）计算器（见下文），并将填好的电子表格（或页面截图）发送给客户服务中心。

The audit time (incl. plan and reporting hours) needed for certification is calculated in accordance with ISO/IEC 27006 (section 9.1.4 and Annex B).认证所需的审核时间（包括计划和报告时间）是根据 ISO/IEC 27006（第 9.1.4 节和附录 B）计算得出的。

The on-site audit duration must be at least 70% of the total audit time. For the calculation of the on-site audit time, the **quality**austria IMS Calculator should be used (FO_25_03_17e_IMS Calculator).现场审核时长必须至少占总审核时间的 70%。在计算现场审核时间时，应使用 **quality**austria 的综合管理体系（IMS）计算器（FO_25_03_17e_IMS 计算器）。

Any factors to be taken into account for increasing or reducing the audit duration will have to be taken from ISO/IEC 27006:2015.任何会导致审核时长增加或减少的需考虑因素，都必须依据 ISO/IEC 27006:2015 来确定。

The time allocated shall also consider the **following factors which relate to the complexity** of the ISMS and therefore to the effort needed to audit the ISMS:
所分配的时间还应考虑以下与信息安全管理体系（ISMS）的复杂程度相关的因素，因而也与审核该信息安全管理体系所需的工作量相关：

a) complexity of the ISMS (e.g. criticality of information, risk situation of the ISMS, etc.);
信息安全管理体系的复杂程度（例如，信息的关键程度、信息安全管理体系的风险状况等）
b) the type(s) of business performed within scope of the ISMS;
在信息安全管理体系范围内开展的业务类型
c) previously demonstrated performance of the ISMS;信息安全管理体系先前已展现出的绩效
d) extent and diversity of technology utilized in the implementation of the various components of the ISMS (e.g. number of different IT platforms, number of segregated networks); 在实施信息安全管理体系的各个组成部分时所使用技术的范围和多样性（例如，不同的信息技术平台的数量、隔离网络的数量）
e) extent of outsourcing and third party arrangements used within the scope of the ISMS;
在信息安全管理体系范围内外包和第三方合作安排的程度
f) extent of information system development;信息系统开发的程度
g) number of sites and number of Disaster Recovery (DR) sites;
场所的数量以及灾难恢复（DR）场所的数量
h) for surveillance or re-certification audit: The amount and extent of change relevant to

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

the ISMS in accordance with ISO/IEC 17021-1, 8.5.3.对于监督审核或再认证审核：根据 ISO/IEC 17021-1 第 8.5.3 条，与信息安全管理体系相关的变更的数量和程度

Annex C of ISO/IEC 27006 provides examples how these different factors can be taken into account when calculating audit time.
ISO/IEC 27006 的附录 C 提供了在计算审核时间时如何考虑这些不同因素的示例。

Additional example factors requiring **additional audit time** are:
需要额外审核时间的其他示例因素包括：

- complicated logistics involving more than one building or location in the scope of the ISMS; 涉及信息安全管理体系范围内不止一栋建筑物或一个地点的复杂物流情况
- staff speaking more than one language (requiring interpreter(s) or preventing individual auditors from working independently) or documentation provided in more than one language;员工使用不止一种语言（需要口译员或导致单个审核员无法独立开展工作），或者提供的文件使用不止一种语言
- activities that require visiting temporary sites to confirm the activities of the permanent sites(s) whose management system is subject to certification (see paragraph below next list);需要访问临时场所，以确认其管理体系正在接受认证的永久场所的活动（请见下一条目下的段落）
- high number of standards and regulations that apply to the ISMS.
  适用于该信息安全管理体系的大量标准和法规

Example factors permitting **less audit time** are 允许减少审核时间的示例因素包括：

- no/low risk product/processes; 无风险或低风险的产品 / 流程
- processes involving a single general activity (e.g. service only); 涉及单一常规活动的流程（例如，仅提供服务）
- high percentage of persons doing work under the organization's control performing the same tasks; 在组织控制下从事相同任务的人员比例较高
- prior knowledge of the organization (for example, if the organization has already been certified to another standard by the same certification body);对该组织的预先了解（例如，如果该组织已由同一认证机构依据另一标准进行了认证）
- high client preparedness for certification (for example, already certified or recognized by another 3rd party scheme); 客户对认证的准备程度很高（例如，已通过其他第三方认证计划获得认证或认可）
- high maturity of the management system in place.现有管理体系的成熟度很高

In situations where the certification client or certified organization provides their product(s) or service at **temporary sites** it is important that evaluations of such sites are incorporated into the certification audit and surveillance programs.在认证客户或已获认证的组织在临时场所提供其产品或服务的情况下，将对这些临时场所的评估纳入认证审核和监督计划是非常重要的。

In accordance with ISO/IEC 27006:2015, the following audit times apply for initial certifications, surveillance and re-certification audits, including preparation, implementation and report:
根据 ISO/IEC 27006:2015，以下审核时间适用于初次认证、监督审核和再认证审核，包括审核准备、实施和报告工作：

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

Table 表格 B.1
Determination of Audit Time 确定审核时间

Effective Number of Personnel 有效人数	Audit Duration Stage 1 + Stage 2 (days including reporting time) 审核时长（包括报告时间在内的天数）：第一阶段 + 第二阶段	Onsite Audit time (Hours) = N_{days}*0,7*8 现场审核时间（小时）= $N_{天数}$*0,7*8	Stage 1 第一阶段	Stage 2 第二阶段	Surveillance 监督审核	Re-Certification 再认证审核
1~10	5,0	28	6	22	9	19
11~15	6,0	34	6	28	11	22
16~25	7,0	39	6	33	13	26
26~45	8,5	48	6	42	16	32
46~65	10,0	56	8	48	19	37
66~85	11,0	62	8	54	21	41
86~125	12,0	67	8	59	22	45
126~175	13,0	73	8	65	24	49
176~275	14,0	78	10	68	26	52
276~425	15,0	84	10	74	28	56
426~625	16,5	92	10	82	31	62
626~875	17,5	98	10	88	33	65
876~1175	18,5	104	12	92	35	69
1176~1550	19,5	109	12	97	36	73
1551~2025	21,0	118	12	106	39	78
2026~2675	22,0	123	12	111	41	82
2676~3450	23,0	129	16	113	43	86
3451~4350	24,0	134	16	118	45	90
4351~5450	25,0	140	16	124	47	93
5451~6800	26,0	146	16	130	49	97
6801~8500	27,0	151	16	135	50	101
8501~10700	28,0	157	16	141	52	105
> 10,700	Follow progression above 请遵循上述步骤					

The table above defines the minimum onsite audit time per audit. This corresponds to 70% of the total audit time.上表规定了每次审核的最低现场审核时间。该时间相当于总审核时间的70%。

When planning your audit, be sure to achieve the correct total audit time, including preparation, document review and audit report time.在策划审核工作时，请务必确保达到正确的总审核时间，其中包括审核准备、文件评审以及审核报告撰写的时间。

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

In case of simple IS-Systems with low IS-risks audit time may be reduced. **The audit time provided in the audit time chart shall not be reduced by more than 30 %** (see also IMS-calculator).对于信息安全风险较低的简单信息安全系统，审核时间可以缩短。但审核时间图表中所规定的审核时间缩短幅度不得超过 30%（另请见综合管理体系计算器的相关内容）。

3.2 Specifics for multi-site audits 多现场审核的具体细节

The number of auditor days per site, including the central office, shall be calculated for each site. Reductions may be applied to take into account the parts of the audit that are not relevant to the central office or the local sites. Reasons for the justification of such reductions shall be recorded by the certification body.应针对包括总部办公室在内的每个场所计算审核人日数。考虑到部分审核内容可能与总部办公室或当地场所不相关，可对审核人日数进行削减。认证机构应记录此类削减的合理理由。
The reduction shall be done with IAF MD1 and is limited to 20% per site.
削减应依据国际认可论坛（IAF）强制性文件 1（IAF MD1）进行，且每个场所的削减幅度限制在 20% 以内。

3.3 Sampling in Multi-site audits 多现场审核的抽样

There are no ISMS specific criteria to decide if sampling is allowed (IAF MD1 contains all requirements from ISO/IEC 27006:2015).对于是否允许采用抽样方法，目前并无信息安全管理体系（ISMS）方面的特定标准（国际认可论坛强制性文件 1（IAF MD1）包含了 ISO/IEC 27006:2015 中的所有要求）。

However, to choose the correct samples, there are specific criteria. In Integrated multi-site audits, the auditor might need to choose different locations than for other models, based on the following considerations.然而，为了选择合适的样本，存在一些特定标准。在综合多场所审核中，审核员可能需要基于以下考虑，选择与其他模式不同的场所进行审核。

1) Before deciding to take a sampling approach **analyse the difference between sites** such that an adequate level of sampling is determined. The activities at each site must be recorded in the FO_25_03_17 audit program. 在决定采用抽样方法之前，需分析各场所之间的差异，从而确定适当的抽样水平。每个场所的活动都必须记录在 FO_25_03_17 审核计划中。
2) A representative number of sites should be sampled taking into account:
应抽取具有代表性数量的场所样本，同时需考虑以下因素：
1) the results of internal audits of the head office and the sites;
总部办公室和各场所的内部审核结果
2) the results of management review;
管理评审的结果
3) variations in the size of the sites;
各场所规模的差异
4) variations in the business purpose of the sites;
各场所业务目的的差异
5) complexity of the information systems at the different sites;
不同场所信息系统的复杂程度
6) variations in working practices;
工作实践的差异
7) variations in activities undertaken;
所开展活动的差异
8) variations of design and operation of controls;
控制措施的设计和运行方面的差异
9) potential interaction with critical information systems or information systems processing sensitive information;
与关键信息系统或处理敏感信息的信息系统的潜在交互情况

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

10) any differing legal requirements;
任何不同的法律要求
11) geographical and cultural aspects;
地理和文化方面的因素
12) risk situation of the sites;
各场所的风险状况
13) information security incidents at the specific sites.
特定场所发生的信息安全事件

3) **Every site** included in the ISMS which is subject to **significant risks is audited prior to initial certification**. This means for the initial certification you might need to consider more samples than in later audits.在初次认证之前，应对信息安全管理体系中存在重大风险的每个场所进行审核。这意味着，与后续审核相比，初次认证时可能需要考虑抽取更多的样本。

4) **In the case of a nonconformity being observed, either at the head office or at a single site, the corrective action procedure applies to the head office and all sites covered by the certificate. In the FO_27_01_33 action list your verification needs to include a statement on this.**如果在总部办公室或单个场所发现了不符合项，纠正措施程序应适用于总部办公室以及证书涵盖的所有场所。在 **FO_27_01_33** 整改措施清单中，验证工作需要包含关于这一点的说明。

5) The audit shall address the client's **head office** activities to ensure that a single ISMS applies to all sites and **delivers central management at the operational level**. The audit shall address all the issues outlined above. Plan sufficient time at the head office and document your findings in the checklist.审核应涵盖客户总部办公室的活动，以确保单一的信息安全管理体系适用于所有场所，并在运营层面提供集中管理。审核应处理上述所有问题。在总部办公室安排足够的审核时间，并将你的审核发现记录在检查表中。

3.4 Time needed for combined audits 联合审核所需时间

The ISMS audit may be combined with audits of other management systems, provided that it can be demonstrated that the audit satisfies all requirements for certification of the ISMS.信息安全管理体系（ISMS）审核可以与其他管理体系的审核相结合，前提是能够证明该审核满足信息安全管理体系认证的所有要求。

For calculating of the audit time for all other management systems IAF mandatory document for the application of ISO/IEC 17021 for audits of integrated management systems (IAF MD 11, Issue 1) shall be applied. Also see RE_25_03_01e_minimum audit time.
对于计算所有其他管理体系的审核时间，应应用国际认可论坛（IAF）关于在综合管理体系审核中应用 ISO/IEC 17021 的强制性文件（IAF MD 11，第 1 版）。另请参阅 RE_25_03_01e 最低审核时间

For calculating the on-site audit time incl., the time for integrated audits, the **quality**austria IMS Calculator may be used (FO_25_03_17e_IMS Calculator).在计算现场审核时间（包括综合审核的时间）时，可以使用 **quality**austria 的综合管理体系（IMS）计算器（FO_25_03_17e_IMS 计算器）

3.5 Remote audit 远程审核

Remote auditing techniques can be used. Remote audit planning will be carried out in accordance with RE_25_03_03e "Remote assessment", however remote auditing **techniques cannot be more than 30% of the on-site audit time**.可以采用远程审核技术。远程审核策划将根据 RE_25_03_03e 远程评估来制定，不过，远程审核技术的使用时间不得超过现场审核时间的 30%。

If more than 30 % remote audit time are planned, the auditor has to justify the audit plan and Quality Austria needs to obtain **specific approval from the accreditation body** prior to its implementation!!!如果策划的远程审核时间超过 30%，审核员必须对审核计划作出合理说明，并且 Quality Austria 需要在实施该计划之前获得认可机构的明确批准！！！

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

3.6 Registration for certification 注册和认证

Registration will be done by using the registration form FO_25_03_29e "Information offer making IS" and while considering the General Terms and Conditions of Quality Austria according to the general process requirements for this process.注册将通过使用注册表格 FO_25_03_29e《信息安全相关信息提供表》来完成，并且在注册时需根据此流程的一般流程要求，考虑 Quality Austria 的通用条款和条件。

3.7 Fees 费用

The Fee Model is implemented in **quality**austria GPS and released by the product expert and **quality**austria management. 收费模式已在 **quality**austria 的 GPS 中实施，并由产品专家和 **quality**austria 管理层批准。

4. Requirements placed on the auditors and technical experts 对审核员和技术专家的要求

4.1 Competence Requirements 能力要求

Basis is the qualification process as described in the Regulation RE_05_01_05_01e_Qualification Guidelines for **quality**austria auditors in general, especially section 2 (schematic overview of authorization steps), 4 and 5 apply. 其基础是 **quality**austria 审核员通用资质评定程序，具体内容如法规 RE_05_01_05_01e **quality**austria 审核员资质评定指南所述，尤其是其中的第 2 部分（授权步骤示意图）、第 4 部分和第 5 部分适用。

Due to the sector specific requirements, the qualification requirements differ to other models, as described below (esp. section 3 of RE_05_01_05_01e_Qualification Guidelines for **quality**austria auditors does NOT apply).由于存在特定行业的要求，资质评定要求与其他模式有所不同，如下所述（特别是法规 RE_05_01_05_01e **quality**austria 审核员资质评定指南的第 3 部分不适用）。

Language requirements: Auditors need to have B1 English skills, as key documents are kept in English language. Audits can be carried out and documented in the respective local language.
语言要求：审核员需具备英语 B1 水平，因为关键文件均为英文。审核工作可以使用相应的当地语言开展，并以该语言记录审核情况。

For being authorized as auditor, persons can choose between two options:
对于想要获得审核员授权的人员，可以在以下两种选择中进行抉择：

1) Full authorization: The auditor is capable to audit all technical areas of ISO/IEC 27002 all requirements of ISO/IEC 27006 apply
全面授权：该审核员有能力审核 ISO/IEC 27002 的所有技术领域，需满足 ISO/IEC 27006 的所有要求
2) MS - Authorization: Auditors are limited to audit the management system relevant aspects and the following controls of ISO/IEC 27002:
管理体系授权：审核员仅限于审核与管理体系相关的方面，以及 ISO/IEC 27002 中的以下控制措施：
   - Information Security Policies 信息安全策略
   - Organisation of Information Security 信息安全组织
   - Human Resource Security 人力资源安全
   - Media Handling 媒介管理
   - Compliance 合规性

And shall work **as co-auditor** together with an auditor having a full authorization in a team.
并且，此类审核员应在团队中与拥有全面授权的审核员一同作为审核组员开展工作。

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

The requirements of ISO/IEC 27006/ IAF MD 13 (Annex A) are implemented as follows:
ISO/IEC 27006 / 国际认可论坛（IAF）强制性文件 13（附录 A）的要求实施方式如下：

Nr.	Clause 条款 ISO/IEC 27006/ IAF MD 13	Content 内容	Competence Requirement FA 全面授权的能力要求	Competence Requirement MS-A 管理体系授权的能力要求
1	ISO/IEC 27006, 7.1.2.1.1	General Requirements 一般要求	4-year Work experience in IT wherefrom two in IS alternatively 具有 4 年 IT 领域工作经验，其中 2 年在信息安全（IS）领域；或者 • specialized degree in information security or related areas and two years of work experience or 拥有信息安全或相关领域的专业学位，以及 2 年工作经验；或者 • work experience in related area and CISSP examination 在相关领域有工作经验，并通过了 CISSP（注册信息系统安全专家）考试	• 4-year Work experience in IT and/or IS related areas and 具备 4 年 IT 和 / 或 IS 相关领域的工作经验 • Completion of CISSP course or equivalent 完成 CISSP 课程或同等课程
2	ISO/IEC 27006, 7.1.2.1.2	Information security management terminology, principles, practices and techniques 信息安全管理术语、原则、实践和技术	4-year Work experience alternatively 4 年工作经验，或者 • specialized degree in information security or related areas and two years of work experience or 拥有信息安全或相关领域的专业学位以及 2 年工作经验 • work experience in related area and CISSP examination 在相关领域有工作经验并且通过了注册信息系统安全专家（CISSP）考试	• 4-year Work experience in IT and/or IS related areas and • Completion of CISSP course or equivalent 在信息技术（IT）和 / 或信息安全（IS）相关领域有 4 年工作经验，并完成注册信息系统安全专家（CISSP）课程或同等课程
3	ISO/IEC 27006, 7.1.2.1.3 / IAF MD13 annex A, A4	Information security management system standards and normative documents 信息安全管理体系标准和规范性文件	CIS ISMS certificate or equivalent CIS 信息安全管理体系证书或同等证书	CIS ISMS certificate or equivalent CIS 信息安全管理体系证书或同等证书
4	ISO/IEC 27006, 7.1.2.1.4	Business management practices 业务管理实践	CIS ISMS certificate or equivalent CIS 信息安全管理体系证书或同等证书	CIS ISMS certificate or equivalent CIS 信息安全管理体系证书或同等证书

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

5	ISO/IEC 27006, 7.1.2.1.5 / IAF MD13 Annex A, A7	Client Business Sector. 客户业务领域	Work experience (at least 2 years in the specific sector or similar industry – ISO 9001 groups of codes apply according to AA L08) alternatively 2 audits in this sector or Sector specific training 工作经验（至少在特定领域或类似行业有 2 年工作经验 —— 根据 AA L08 适用 ISO 9001 代码分组），或者在该领域进行过 2 次审核，或者接受过特定领域的培训	Work experience (at least 2 years in the specific sector or similar industry – ISO 9001 groups of codes apply according to AA L08) alternatively 工作经验（至少在特定行业或类似行业拥有两年工作经验 —— 根据 AA L08 标准，适用 ISO 9001 编码分组）；或者可选择以下两种情况之一 • 2 audits in this sector or 在该行业进行过两次审核，或 • Sector specific training 行业特定培训
6	ISO/IEC 27006, 7.1.2.1.6 / IAF MD 13 Annex A, A 7	Client products, processes and organization 客户产品、流程和组织	Work experience (at least 2 years in the specific sector or similar industry – ISO 9001 groups of codes apply according to AA L08) alternatively 工作经验（至少在特定领域或类似行业有两年工作经验 —— 根据 AA L08，适用 ISO 9001 代码分组），或者 • 2 audits in this sector or 在该领域进行过两次审核，或 • Scope specific training 接受过针对该业务范围的特定培训	Work experience (at least 2 years in the specific sector or similar industry – ISO 9001 groups of codes apply according to AA L08) alternatively 工作经验（至少在特定行业或类似行业有两年工作经验 —— 根据 AA L08，适用 ISO 9001 代码分组），或者可选择以下情况之一 • 2 audits in this sector or 在该行业进行过两次审核，或 • Scope specific training 业务范围的特定培训
7	ISO/IEC 27006, 7.1.2.2	Competence requirements for leading the ISMS audit team 领导信息安全管理体系（ISMS）审核团队的能力要求	CIS IS auditor course or **quality**austria auditor certificate CIS 信息系统审核员课程或 **quality**austria 审核员证书	CIS IS auditor course or **quality**austria auditor certificate CIS 信息系统审核员课程或 **quality**austria 审核员证书
8	ISO/IEC 27006, 7.2.1.1	professional education or training to an equivalent level of university education 达到相当于大学教育水平的专业教育或培训	Bachelor degree, M.Sc. or other (NQR Level 6) 学士学位、理学硕士学位或其他（NQR 六级水平）	Bachelor degree, M.Sc. or other (NQR Level 6) 学士学位、理学硕士学位或其他（NQR 六级水平）
9		Four years full time practical workplace experience in information technology of which at least two years are in a role or function relating to information security;四年全日制的信息技术领域实际工作经验，其中至少两年从事与信息安全相关的岗位或职能工作	4-year Work experience in IT wherefrom two in IS alternatively 四年信息技术（IT）领域的工作经验，其中两年需在信息安全（IS）领域；或者 • specialized degree in information security or related areas and two years of work experience or 拥有信息安全或相关领域的专业学位，以及两年工作经验或 • work experience in related area and CISSP examination 具备相关领域的工作经验，并通过注册信息系统安全专家（CISSP）考试	• 4-year Work experience in IT and/or IS related areas and 在信息技术（IT）和 / 或信息安全（IS）相关领域拥有四年工作经验，并且 • Completion of CISSP course or equivalent 完成了注册信息系统安全专家（CISSP）课程或同等课程

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

10		successfully completed at least five days of training, the scope of which covers ISMS audits and audit management 已成功完成至少为期五天的培训，该培训的范围涵盖信息安全管理体系（ISMS）审核以及审核管理	• CISSP examination and 通过注册信息系统安全专家（CISSP）考试 • CIS ISMS course and 完成 CIS 信息安全管理体系（ISMS）课程 • CIS IS-Auditor course or **quality**austria auditor certificate 完成 CIS 信息系统审核员课程；或者持有 **quality**austria 审核员证书	• Completion of CISSP course or equivalent and 完成注册信息系统安全专家（CISSP）课程或同等课程 • CIS ISMS course and 完成 CIS 信息安全管理体系（ISMS）课程 • CIS IS-Auditor course or **quality**austria auditor certificate 完成 CIS 信息系统审核员课程；或者持有 **quality**austria 审核员证书
11	ISO/IEC 27006, 7.2.1.1d); also see amendement 另请参阅修正	has gained experience of auditing ISMS priorto acting as an auditor performing ISMS audits. This experience shall be gained by performing asan auditor-in-training monitored by an ISMS evaluator (see ISO/IEC 17021-1:2015, 9.2.2.1.4) in at least one ISMS 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 ISMS on-site audit days and performed in the last 5 years. The participation shall include review of documentation and risk assessment, implementation assessment and audit reporting.在担任进行信息安全管理体系（ISMS）审核的审核员之前，已积累了 ISMS 审核方面的经验。该经验应通过作为实习审核员在 ISMS 评估员的监督下（见 ISO/IEC 17021-1:2015，9.2 2.1.4）开展工作来获取，且至少参与一次 ISMS 初次认证审核（第一阶段和第二阶段）或再认证审核，以及至少一次监督审核。这种经验应在至少 10 个 ISMS 现场审核日中获取，并且是在过去 5 年内完成的。参与工作应包括文件评审、风险评估、实施情况评估以及审核报告的编制。	As observer at least one ISMS initial certification audit (stage 1 and stage 2) or re-certification and at least one surveillance audit.作为观察员，至少参与一次信息安全管理体系（ISMS）初次认证审核（第一阶段和第二阶段）或再认证审核，以及至少一次监督审核。 The participation shall include review of documentation and risk assessment, implementation assessment and audit reporting.参与工作应包括对文件的评审、风险评估、实施情况评估以及审核报告的撰写。	As observer at least one ISMS initial certification audit (stage 1 and stage 2) or re-certification and at least one surveillance audit.作为观察员，至少参与一次信息安全管理体系（ISMS）初次认证审核（第一阶段和第二阶段）或再认证审核，以及至少一次监督审核。 The participation shall include review of documentationand risk assessment, implementation assessment and audit reporting.参与工作应包括对文件的评审、风险评估、实施情况评估以及审核报告的撰写。

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

12		Relevant and current experience 相关且最新的经验	CISSP certificate not older than three years（持有）不超过三年的注册信息系统安全专家（CISSP）证书	CISSP course not older than three years 不超过三年的注册信息系统安全专家（CISSP）课程
13		keeps current knowledge and skills in information security and auditing up to date through continual professional development 通过持续的专业发展，使信息安全和审核方面的知识与技能保持最新状态	Participate in yearly IS-calibration meetings 参加年度信息安全（IS）校准会议	Participate in yearly IS-calibration meetings 参加年度信息安全（IS）校准会议
14	ISO/IEC 27006, 7.2.1.2	Selecting auditors for leading the team 挑选负责领导团队的审核员	Participate in at least three ISMS audits as auditor A2 作为 A2 审核员参与至少三次信息安全管理体系（ISMS）审核	Participate in at leastthree ISMS audits as auditor A2 作为 A2 审核员参与至少三次信息安全管理体系（ISMS）审核
15	IAF MD13 annex A (A1, A2, A3, A6	knowledge of terminology and principles including ISO/IEC 27000, practices, techniques, risk assessment and risk management included in ISO/IEC 27007, ISO/IEC TS 27008, ISO/IEC 17021-1, ISO/IEC 27006 and SO/IEC 27005. 掌握包括 ISO/IEC 27000 系列标准中的术语和原则、实践方法、技术，以及 ISO/IEC 27007、ISO/IEC TS 27008、ISO/IEC 17021 - 1、ISO/IEC 27006 和 ISO/IEC 27005 中所涵盖的风险评估与风险管理知识	CIS ISMS course CIS 信息安全管理体系（ISMS）课程	CIS ISMS course CIS 信息安全管理体系（ISMS）课程
16	IAF MD13 annex A, A5 / ISO/IEC 27006, A 3.1	General legal and regulatory requirements related to ISMSs (intellectual property, content, protection and retention of organizational records, data protection and privacy, regulation of cryptographic controls, electronic commerce, electronic and digital signatures, workplace surveillance, telecommunications interception and monitoring of data (e.g. e-mail), computer abuse, electronic evidence collection, penetration testing, international and national sector-specific requirements (e.g. banking).	CIS ISMS course CIS 信息安全管理体系（ISMS）课程	CIS ISMS course CIS 信息安全管理体系（ISMS）课程

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

		与信息安全管理体系（ISMSs）相关的一般法律和法规要求（包括知识产权、内容保护以及组织记录的保存、数据保护和隐私、加密控制的监管、电子商务、电子和数字签名、工作场所监控、电信拦截和数据监测（如电子邮件）、计算机滥用、电子证据收集、渗透测试、国际和国内特定行业要求（如银行业）		
17	IAF MD 26:2023, 4.2 / ISO/IEC 27002:2022 / ISO/IEC 27001:2022/ ISO/IEC 27006:2015, 7.1.2.1.3 b).	New controls contained in ISO/IEC 27002:2022, and their Implementation ISO/IEC 27002:2022 中包含的新控制及其实施	CIS ISMS Auditor course or **quality**austria auditor certificate CIS ISMS 审核员课程或 **quality**austria 审核员证书	CIS ISMS Auditor course or **quality**austria auditor certificate CIS ISMS 审核员课程或 **quality**austria 审核员证书

Exceptionally, shorter duration of experience or experiences in the fields other than information security may be considered as appropriate. In such cases, the candidate shall provide evidence that the experience is equivalent. 特殊情况下，较短时长的工作经验或信息安全领域以外的工作经验，若合理也可予以考虑。在此类情形下，候选人应提供证据证明其经验具有同等效力。

IMPORTANT: A self-declaration of the auditor to demonstrate competence without appropriate verification documents is insufficient. 重要提示：审核员仅作自我声明以证明其具备相应能力，而无适当的验证文件，这是不充分的。

A. Requirements for Observers 观察员要求:

Full authorization (for details and alternatives, see above):
全面授权（有关详细信息和替代方案，请见上文）：

1) University degree 大学学位
2) 4-year Work experience in IT wherefrom two in IS (or equivalent, see above)
在信息技术（IT）领域有四年工作经验，其中两年在信息安全（IS）领域（或同等情况，见上文）
3) Completion of CIS ISMS certificate (or equivalent)
获得 CIS 信息安全管理体系（ISMS）证书（或同等证书）
4) Completion of CIS IS auditor certificate (or equivalent)
获得 CIS 信息系统（IS）审核员证书（或同等证书）

MS authorization (for details and alternatives, see above):
MS 授权（有关详细信息和替代方案，请见上文）：

1) University degree 大学学位
2) four years IT/IS related workplace experience (or equivalent, see above)
四年与信息技术 / 信息安全（IT/IS）相关的工作经验（或同等情况，见上文）
3) CISSP course (not older than three years)
完成注册信息系统安全专家（CISSP）课程（课程完成时间不超过三年）
4) Completion of CIS ISMS certificate (or equivalent)
获得 CIS 信息安全管理体系（ISMS）证书（或同等证书）
5) Completion of CIS IS auditor certificate (or equivalent)
获得 CIS 信息系统（IS）审核员证书（或同等证书）

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

B. Requirements Auditor A2 A2 审核员要求

For Observers to be authorized as A2, the following requirements have to be fulfilled:
对于要被授权为 A2 级审核员的观察员，必须满足以下要求：

1. Initial auditor training at Quality Austria
   在 Quality Austria 参加初级审核员培训
2. Self-study of this Guideline and successful completion of the Moodle test(s) incl. knowledge check ISO/IEC 27001
   自学本指南，并成功完成 Moodle 测试（包括对 ISO/IEC 27001 的知识考核）
3. As observer at least one ISMS initial certification audit (stage 1 and stage 2) or re-certification and positive assessment by a commissioned Auditor A1 (FO_05_01_03_03e_Assessing observers auditors) and at least one surveillance audit.
   作为观察员，至少参与一次信息安全管理体系（ISMS）初次认证审核（第一阶段和第二阶段）或再认证审核，并得到受委托的 A1 级审核员的正面评价（参考文件 FO_05_01_03_03e《评估观察员和审核员》），同时至少参与一次监督审核
4. The total duration of audits should be at least 10 on-site audit days, performed in the last 5 years.审核的总时长应至少为 10 个现场审核日，且这些审核需在过去 5 年内完成
   For MS authorisation, extensive audit experience in other Management System models (esp. ISO 9001, 45001, ISO 22301) as **quality**austria lead auditor can be accepted. Audit experience shall be however at least 20 on-site days.
   对于 MS 授权，作为 **quality**austria 的审核组长，在其他管理体系模式（特别是 ISO 9001、ISO 45001、ISO 22301）中有丰富的审核经验是可以被接受的。不过，审核经验至少应为 20 个现场审核日
   For full authorisation, extensive current system evaluation experience (system analysis, threat analysis, network analysis, incident management, internal audits) can be accepted as equivalent.对于全面授权，当前拥有丰富的体系评估经验（如体系分析、威胁分析、网络分析、事件管理、内部审核等）可被视为具备同等条件

Notes 注意事项:
Auditors who have been appointed as **auditor** for other accredited Certification Bodies (e.g. CIS), can be appointed as A2 auditor, directly.已被其他认可认证机构（如 CIS）任命为审核员的人员，可以直接被任命为 A2 级审核员。

C. Requirements Auditor A1 A1 审核员要求

Note: Auditors with MS-Authorisation cannot get A1 status.
注意事项：获得 MS 授权的审核员无法获得 A1 级资质。

For Auditors A2 to be authorized as Auditor A1, the following requirements have to be fulfilled:
对于 A2 级审核员要获得 A1 级审核员的授权，必须满足以下要求：

1. 3 audits as co-auditor with status A2 以 A2 级审核员身份作为审核组员与 3 次审核

Notes 注意事项:

Auditors who have been appointed as **lead-auditor** for other accredited Certification Bodies (e.g. CIS), can be appointed as A1 auditor, directly. Their first audit for Quality Austria as A1 must be supervised, monitored and evaluated by an appointed **quality**austria A1 Auditor.已被其他认可认证机构（如 CIS）任命为审核组长的人员，可以直接被任命为 A1 级审核员。他们作为 A1 级审核员在 Quality Austria 进行的首次审核，必须由指定的 Quality Austria A1 级审核员进行监督、监控和评估。

4.2 Appointment for an EAC Code EAC 代码的任命

In addition to the application for appointment as an auditor for a specific standard, it is also necessary to apply for which EAC Scope one wishes to be appointed. See

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

FO_05_01_05_02_Application form EAC Scope and RE_05_01_05_12_Approvals EAC Scope.
除了申请被任命为针对特定标准的审核员外，还需要申请希望被任命的欧洲认可合作组织（EAC）的业务范围。请参阅文件 FO_05_01_05_02《EAC 业务范围申请表》以及 RE_05_01_05_12《EAC 业务范围批准书》

For the evaluation of different professional experience and training, the EAC scopes were divided on a risk-based approach into groups (A, B, C) that can be viewed as "related" for ISO/IEC 27001. E.g. Group A has a high regulatory background. 为了评估不同的专业经验和培训情况，基于风险的方法，EAC 的业务范围被划分为 A、B、C 等组，对于 ISO/IEC 27001 标准而言，这些组可被视为"相关的"。例如，A 组具有较高的监管背景。
Industry group C (non-specific / generic) does not have any special industry specifics, so that it can be properly audited by any appointed auditor. C 行业组（非特定 / 通用）不具有任何特殊的行业特性，因此，任何被任命的审核员都可以对其进行适当的审核。

№	Industry 行业	EAC Scopes EAC 范围	Group 组别
1	Coke and Refined Petroleum Products 焦炭和精炼石油产品	10	A
2	Nuclear Fuel 核燃料	11	A
3	Chemicals, Chemical Products and Fibres 化学品、化学制品及纤维	12	A
4	Pharmaceuticals 药品；药物	13	A
5	Ship building 造船	20	A
6	Aerospace 航空	21	A
7	Mining and Quarrying, Extraction of crude petroleum and natural gas 采矿和采石，原油和天然气的开采	2	B
8	Basic metals and Fabricated Metal Products 基础金属及金属制品	17	B
9	Machinery and Equipment 机械设备	18	B
10	Electrical and Optical Equipment, Communication Technology, Medical Devices 电气和光学设备、通信技术、医疗器械	19	B
11	Other Transport Equipment, Manufacture of motor vehicles / parts of motor vehicles 其他运输设备，汽车制造/汽车零部件	22	B
12	Recycling 回收利用	24	B
13	Electricity supply 电力供应	25	B
14	Gas supply 燃气供应	26	B
15	Water supply 供水	27	B
16	Construction 建造	28	B
17	Transport, Storage and Communication 运输、仓储和通信	31	B
18	Financial Intermediation, Real Estate, Renting 金融中介、房地产、租赁	32	B

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

19	Information Technology 信息技术	33	B
20	Public administration 公共管理	36	B
21	Agriculture, Hunting, Forestry & Fishing 农业、狩猎、林业和渔业	1	C
22	Food products, Beverages and Tobacco 食品、饮料和烟草	3	C
23	Textile and Textile Products 纺织及纺织产品	4	C
24	Leather and Leather Products 皮革及皮革制品	5	C
25	Wood and Wood Products 木材及木制品	6	C
26	Pulp, Patper and Paper Products 纸浆、纸张和纸制品	7	C
27	Publishing Companies 出版公司	8	C
28	Printing Companies 印刷公司	9	C
29	Rubber and Plastic Products 橡胶和塑料制品	14	C
30	Non-metallic Mineral Products 非金属矿物制品	15	C
31	Concrete, Cement, Lime, Plater etc. 混凝土、水泥、石灰、灰泥等	16	C
32	Manufacturing not elsewhere classified 其他未分类制造业	23	C
33	Wholesale and retail trade; repair of motor vehicles, motorcycles and personal and household goods 批发和零售业；汽车、摩托车以及个人和家庭用品修理业	29	C
34	Hotels and Restaurants 宾馆和餐馆	30	C
35	Engineering Services 工程服务	34	C
36	Other Services; business, management and tax constultancy, Technical, physical and chemical tesing and analysis 其他服务；商业、管理和税务咨询，技术、物理和化学测试与分析	35	C
37	Education 教育	37	C
38	Health and Social Work, Human health activities, Veterinary activities 健康和社会工作，人类健康活动，兽医活动	38	C
39	Other Social Services; Sewage and refuse disposal 其他社会服务；污水和垃圾处理	39	C

4.3 Impartiality 公正性

Quality Austria auditors shall be impartial and free from engagements and influences which could affect their objectivity, and in particular shall not be:

Quality Austria 的审核员应保持公正，且不受可能影响其客观性的业务委托和影响因素的干扰，尤其不得有以下行为：

a) involved in the stages of the client product or service life cycle
参与客户产品或服务生命周期的各个阶段

b) involved in the design, implementation or maintenance of the information security management systems being audited

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

参与正在接受审核的信息安全管理体系的设计、实施或维护工作

c) an authorized representative of the client organization, nor represent the parties engaged in these activities
担任客户组织的授权代表，也不得代表参与这些活动的各方

The situations hereafter are examples where impartiality is compromised in reference to the criteria defined in a) to c):
以下这些情况是参照上述 a) 至 c) 项所定义的标准，表明公正性受到损害的例子：

a) the auditor having a financial interest in the client organization being audited (e.g., holding stock in the organization)审核员在被审核的客户组织中存在经济利益关系（比如，持有该组织的股票）
b) the auditor being employed currently by a similar company 审核员目前受雇于一家与之类似的公司
c) the auditor being a member of staff from a research institute or a consultant having a commercial contract or equivalent interest with the client or similar company 审核员是某研究机构的一名工作人员，或者是与客户或类似公司签有商业合同或存在同等利益关系的顾问

4.4 Maintenance of competence 维持能力

The general **quality**austria procedures shall be applied – see RE_05_01_06_01e_Maintenance of competence for auditors.应采用 Quality Austria 的通用程序 —— 详见文件 RE_05_01_06_01e 审核员能力维持

In addition, each auditor has to participate in the yearly calibration regarding ISO/IEC 27001. In addition, further training is expected. Participation in at least 2 days of further education (e.g. CIS Forum) in 3 years is a minimum requirement.此外，每位审核员都必须参加关于 ISO/IEC 27001 标准的年度校准活动。另外，还要求参加进一步的培训。最低要求是在三年内至少参加为期两天的进修学习（例如 CIS 论坛相关活动）。

5. Conducting audits 执行审核

Unless stated differently, audits in all respects will be conducted analogously to the **quality**austria procedures as defined for ISO 9001.除非另有规定，否则所有方面的审核都将按照 Quality Austria 针对 ISO 9001 所规定的程序类似地进行。

5.1 Specifics 具体内容

Before the certification audit, the certification body shall ask the client to provide ISMS data by using the Quality Austria form FO 27_01_210 ISMS_Stage1_evidences.在进行认证审核之前，认证机构应要求客户使用 Quality Austria 的表格 FO 27_01_210 信息安全管理体系（ISMS）第一阶段证据表来提供信息安全管理体系的数据。
The certification body also shall ask the client to report if any ISMS related information (such as ISMS 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. 认证机构还应要求客户报告，是否存在任何与信息安全管理体系相关的信息（例如信息安全管理体系记录，或有关控制措施的设计和有效性的信息），因包含机密或敏感信息而无法提供给审核团队进行审查。
The certification body shall determine whether the ISMS can be adequately audited in the absence of such information. If the certification body concludes that it is not possible to adequately audit the ISMS 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. 认证机构应确定在缺少此类信息的情况下，是否仍能够对信息安全管理体系进行充分审核。如果认证机构得出结论，认为若不审查所识别出的机密或敏感信息，就无法对信息安全管理体系进行充分审核，那么它应告知客户，在获得适当的查阅安排之前，无法进行认证审核。

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

For the audit stage 1 and audit stage 2, the corresponding ISO/IEC 27001 checklists (stage 1 and stage 2) shall be used:对于第一阶段审核和第二阶段审核，应使用相应的 ISO/IEC 27001 检查表（第一阶段和第二阶段）：

Stage 1 第一阶段:

- CL_27_01_185e_Stage1_27001
- FO 27_01_210 ISMS_Stage1_evidences 信息安全管理体系（ISMS）第一阶段证据表

Stage 2 第二阶段:

- CL_27_01_186e_ ISO 27001_2013
- CL_27_01_187e_ ISO 27001_2022
- FO 27_01_030e audit and assessment plan (time plan) 审核与评估计划（时间计划）
- FO_27_01_209e Auditreport_MD_ISMS 信息安全管理体系审核报告

5.2 Specialities in ISO/IEC 27001 audits ISO/IEC 27001 审核的具体内容

Special attention shall be paid to the following focus areas according to paragraph 9.4.2 and Annex D „Guidance for review of implemented ISO/IEC 27001:2013 Annex A controls" of ISO/IEC 27006:2015.根据 ISO/IEC 27006:2015 的第 9.4.2 段以及附件 D"已实施的 ISO/IEC 27001:2013 附件 A 控制措施的评审指南"，应特别关注以下重点领域。

5.3 Major nonconformities 严重不符合项

Examples of major nonconformities which require the acceptance and the verification of the effectiveness of correction and corrective actions are as follows:
以下是一些需要接受并验证纠正及纠正措施有效性的严重不符合项示例：

a) failure to fully address applicable requirements and implement an entire process for information security management systems (e.g. failure to have a complaint handling or training system, evidences of management reviews and internal information security management systems audits are missed)
未能全面满足适用要求，且未实施信息安全管理体系的完整流程（例如，没有投诉处理或培训系统，缺失管理评审和内部信息安全管理体系审核的证据）

b) failure to implement applicable requirements for information security management systems
未能实施信息安全管理体系的适用要求

c) failure to implement appropriate corrective action 未能实施适当的纠正措施

d) repeated nonconformities from previous audits 之前审核中出现的重复性不符合项

5.4 Special audits 特殊审核

The activities necessary to perform special audits shall be subject to special provision if a client with a certified ISMS makes major modifications to its system or if other changes take place which could affect the basis of its certification 如果已获得信息安全管理体系（ISMS）认证的客户对其体系进行重大修改，或者发生了其他可能影响其认证基础的变更，那么进行专项审核所必需的相关活动应遵循特殊规定。

6. Certification decision, printing the Certificate and granting Certificates 证书、打印证书和颁发证书

The certification decision shall be based, additionally to the requirements of p. 9.5 .1 ISO/IEC 27006, on the certification recommendation of the audit team as provided in their certification audit report. 除了依据 ISO/IEC 27006 第 9.5.1 条的要求之外，认证决定还应基于审核团队在其认证审核报告中所给出的认证建议。

The persons that take the decision on granting certification should not normally overturn a negative recommendation of the audit team. If such a situation does arise, the veto power shall document and justify the basis for the decision to overturn the recommendation.通常情况下，做出授予认证决定的人员不应推翻审核团队给出的否定建议。如果确实出现了这种情况，拥有否决权的人员应记录并说明推翻该建议的决定所基于的理由。

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

For competence criteria the **quality**austria regulation RE_27_01_063_Approval of Business Transactions applies. In addition, the Veto-reviewer has to be appointed as **quality**austria auditor for ISO/IEC 27001 at least with status "B" (observer). 关于能力标准方面，Quality Austria 的规定 RE_27_01_063《商业交易批准》适用。此外，否决审核人必须被指定为至少具有 "B" 级（观察员）身份的 Quality Austria ISO/IEC 27001 审核员。

Detailed analyse see Annex A. 详细分析见附件 A。

Certification shall not be granted to the client until there is sufficient evidence to demonstrate that arrangements for management reviews and internal ISMS audits have been implemented, are effective and will be maintained. 在有充分证据证明客户已实施了管理评审和信息安全管理体系（ISMS）内部审核的安排，且这些安排是有效的并将持续保持之前，不应授予客户认证。

As for Certificates and for printing Certificates, the procedures as defined for ISO 9001 will generally apply. 至于证书以及证书的打印，通常将适用为 ISO 9001 所规定的程序。

The **quality**austria system certificates according to ISO/IEC 27001 are generally valid for 3 years. 按照 ISO/IEC 27001 颁发的 Quality Austria 体系证书，一般有效期为 3 年。

7. Maintenance and recertification 维持和重新认证

As for maintenance of the Certificate (surveillance activities and recertification), the requirements relating to ISO 9001 will principally apply. 至于证书的维持（监督活动和再认证），与 ISO 9001 相关的要求原则上同样适用。

8. Transition Revision ISO/IEC 27001:2022 向 ISO/IEC 27001:2022 标准的转换修订

Transition audit programme 转换审核方案:

- transition to ISO/IEC 27001:2022 version can occur in frame of re-certification audit. The audit time according with Table B.1
- 向 ISO/IEC 27001:2022 版本的转换可在再认证审核的框架内进行。审核时间依据表 B.1 确定。
- transition to ISO/IEC 27001:2022 version can occur in frame of surveillance audit. The audit time according with Table B.1. plus additional time – min 4 hours (time might be increased depending on complexity of organization/controls).
- 向 ISO/IEC 27001:2022 版本的转换也可在监督审核的框架内进行。审核时间依据表 B.1，再加上额外时间 —— 至少 4 小时（时间可能会根据组织 / 控制措施的复杂程度而增加）。
- The transition can be carried out in a specific transition audit. The audit time – min 4 hours (might be adapted depending on complexity of organization/controls). Such an audit can be carried out remotely, if the transition audit objectives can be met (use checklist for risk assessment).
- 转换可在特定的转换审核中进行。审核时间至少为 4 小时（可能会根据组织 / 控制措施的复杂程度进行调整）。如果能够实现转换审核目标，此类审核可以远程进行（使用风险评估检查表）。

General remark: A pure document review is insufficient – the updated controls shall be reviewed in the surveillance audit.
一般注意事项：单纯的文件评审是不够的 —在监督审核中应评审更新后的控制措施。

Transition Process 转换流程

- Before the transition audit, the certified customer will be asked by the lead auditor to provide a full list of updated controls (FO 27_01_210e_ISMS_Stage1_evidences, section 5).
- 在转换审核之前，审核组长会要求已获认证的客户提供更新后的控制措施的完整清单（FO 27_01_210e_ISMS_第一阶段证据表，第 5 部分）
- The customer should describe the Changed / additional controls in the column "Remarks". Instead of describing the carried out changes in this document, a separate gap analysis can be submitted.

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

- 客户应在“备注”栏中描述已变更 / 新增的控制措施。除了在此文件中描述已实施的变更之外，也可以提交一份单独的差距分析报告

During the transition audit the auditor shall verify and give a written statement in the audit report (please include the four items in section 1.2 "Developments since the last audit"):
在转换审核期间，审核员应进行验证，并在审核报告中给出书面声明（请在 1.2 “自上次审核以来的进展”部分中包含以下四项内容）：

- the gap analysis of ISO/IEC 27001:2022, as well as the need for changes to the client's ISMS;
- 对 ISO/IEC 27001:2022 的差距分析，以及客户信息安全管理体系（ISMS）是否需要变更
- the updating of the statement of applicability (SoA);
- 适用性声明（SoA）的更新情况
- if applicable, the updating of the risk treatment plan;
- （如适用）风险处理计划的更新情况；
- the implementation and effectiveness of the new or changed controls chosen by the clients. and effectiveness of the new or changed controls chosen by the clients.
  客户所选择的新的或已变更的控制措施的实施情况及其有效性。

For each audit with the scope of transition to ISO/IEC 27001:2022 a veto-check shall be carried out. 对于每一次涉及向 ISO/IEC 27001:2022 转换的审核，都应进行否决检查。

The updated certificate can only be issued after successful transition audit to ISO/IEC 27001:2022.只有在成功完成向 ISO/IEC 27001:2022 的转换审核之后，才能颁发更新后的证书。
The certificate ISO/IEC 27001:2022 shall keep the original certification cycle.
ISO/IEC 27001:2022 证书应保持原有的认证周期。

The transfer shall be completed before October 2025, any ISO/IEC 27001:2013 certificate will be withdrawn by 01.11.2025. No initial audits according to ISO/IEC 27001:2013 may start after 1.11.2023. 转换应在 2025 年 10 月之前完成，任何 ISO/IEC 27001:2013 证书将在 2025 年 11 月 1 日被撤销。自 2023 年 11 月 1 日起，不得再开始按照 ISO/IEC 27001:2013 进行的初次审核。

Upgrade Auditor Training 审核员升级培训:

All auditors, whose training was based on ISO/IEC 27001:2013 must complete an upgrade training to the new standard including a knowledge check (20 questions). Auditors can only be appointed to the new version of the standard, when this upgrade training is completed. 所有其培训基于 ISO/IEC 27001:2013 标准的审核员，都必须完成针对新标准的升级培训，其中包括一次知识考核（20 道题目）。只有在完成这项升级培训之后，审核员才能够被委派进行基于新标准的审核工作。

9. Accreditation 认可

Quality Austria is accredited by Accreditation Austria.

Quality Austria 已获得奥地利认可委员会（Accreditation Austria）的认可。

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

10. Enclosures 附件

- FO_25_03_29e_Information_offer_making_IS; FO_25_03_29_Informationen zur Angebotserstellung_IS 信息安全相关报价文件
- FO_25_03_17e_IMS Calculator IMS 计算器
- FO_05_01_03_15e_Qualification form for ISO 27001 ISO 27001 资格认证表格
- RE_05_01_05_01e_Qualification Guidelines for **quality**austria auditors **quality**austria 审核员资格指导方针
- RE_05_01_06_01e_Maintenance of competence for auditors 审核员能力维持
- FO_05_01_03_03e_assessing observers 评估观察员
- FO_05_01_05_02e_Application form EAC Scope EAC 范围申请表
- RE_05_01_05_12_Approvals EAC Scope EAC 范围批准表
- RE_27_01_074e_Certification of multi-site organizations 多场所组织认证文件
- CL_27_01_185e_Stage1_27001 27001 一阶段文件
- FO 27_01_210e_ISMS_Stage1_evidences 信息安全管理体系（ISMS）第一阶段证据表
- CL_27_01_186e_ ISO 27001_2013
- CL_27_01_187e_ ISO 27001_2022
- FO_27_01_209e Auditreport_MD_ISMS; FO_27_01_209 Auditbericht_MP_ISMS
- 信息安全管理体系 MD 审核报告
- FO 27_01_030e audit and assessment plan (time plan) 审核与评估计划（时间计划）
- FO_27_01_033e action list 行动清单
- **quality**austria - Sample Certificate ISO/IEC 27001
- **quality**austria 的 ISO/IEC 27001 证书样本
- ISO/IEC 27001:2013 "Information technology — Security techniques — Information security management systems — Requirements"
- ISO/IEC 27001:2013 信息技术 —安全技术 —信息安全管理体系 —要求
- ISO/IEC 27001:2022 "Information technology — Security techniques — Information security management systems — Requirements"
- ISO/IEC 27001:2022 信息技术 —安全技术 —信息安全管理体系 —要求
- ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Informationsecurity controls
- ISO/IEC 27002:2022 信息安全、网络安全和隐私保护 — 信息安全控制
- ISO/IEC 27006:2015 "Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems"
- ISO/IEC 27006:2015 信息技术 —安全技术 —提供信息安全管理体系审核和认证的机构要求
- IAF Mandatory Document for the Audit and Certification of a Management System Operated by a Multi-Site Organization (IAF MD 1:2023)
- 国际认可论坛（IAF）关于多场所组织管理体系审核和认证的强制文件（IAF MD 1:2023）
- IAF mandatory document for the application of ISO/IEC 17021 for audits of integrated management systems (IAF MD 11:2023)
- IAF 关于将 ISO/IEC 17021 应用于综合管理体系审核的强制文件（IAF MD 11:2023）
- IAF mandatory document for the transition requirements for ISO/IEC 27001:2022 (IAF MD 26:2023)
- IAF 关于 ISO/IEC 27001:2022 转换要求的强制文件（IAF MD 26:2023）

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

11. Annex A: Analyse requirements for Veto-rejection persons 附件 A：分析 veto-否决权的要求

ISO 27006 requirements for veto-persons ISO 27006 对否决人员的要求	Implementation at Quality Austria Quality Austria 的实施情况
7.1.2.4 Competence requirements for reviewing audit reports and making certification decisions 审查审核报告和做出认证决定的人员的能力要求	
7.1.2.4.1 General 总则	
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. 审查审核报告并做出认证决定的人员应具备相应知识，使他们能够验证认证范围的适宜性，以及范围变更及其对审核有效性的影响，特别是接口和依赖关系识别的持续有效性以及相关风险。	Experience in management system certification, 2 Years as Lead Auditor for an ISO 17021-1 related standard or 2 years of full time employment for a ISO 27001 accredited CB 应具备管理体系认证经验，担任与 ISO 17021 - 1 相关标准的审核组长 2 年，或在获得 ISO 27001 认可的认证机构全职工作 2 年
Additionally, the personnel reviewing audit reports and making the certification decisions shall have knowledge of: a) management systems in general; b) audit processes and procedures; c) audit principles, practices and techniques. 此外，审查审核报告并做出认证决定的人员应具备以下方面的知识： a) 一般管理体系； b) 审核流程和程序； c) 审核原则、实践和技术。	CIS IS Manager Certificate and CIS IS Auditor Certificate or **quality**austria auditor certificate 需持有 CIS 信息安全经理证书和 CIS 信息安全审核员证书，或 **quality**austria 审核员证书
7.1.2.4.2 Information security management terminology, principles, practices and techniques 信息安全管理术语、原则、实践和技术	
The personnel reviewing audit reports and making the certification decisions shall have knowledge of: 审查审核报告并做出认证决定的人员应具备以下方面的知识：	
a) the items listed in 7.1.2.1.2 a), c) and d); 7.1.2.1.2 ... shall have knowledge of: a) ISMS specific documentation structures, hierarchy and interrelationships; c) information security risk assessment and risk management; d) processes applicable to ISMS; a) 7.1.2.1.2 中 a)、c) 和 d) 项所列内容：7.1.2.1.2 ..... 应具备以下方面的知识： a) 信息安全管理体系（ISMS）特定的文件结构、层次关系和相互关系； c) 信息安全风险评估和风险管理； d) 适用于信息安全管理体系的流程	CIS IS Manager Certificate 需持有 CIS 信息安全经理证书
b) legal and regulatory requirements relevant to information security.	
7.1.2.4.3 Information security management system standards and normative documents 信息安全管理体系标准和规范性文件	
Personnel reviewing audit reports and making certification decisions shall have knowledge of: a) relevant ISMS standards and other normative documents used in the certification process. 审查审核报告并做出认证决定的人员应具备以下方面的知识： a) 认证过程中使用的相关信息安全管理体系标准和其他规范性文件	CIS IS Manager Certificate 需持有 CIS 信息安全经理证书

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

7.1.2.4.4 Client business sector 客户业务领域 Personnel reviewing audit reports and making certification decisions shall have knowledge of: a) generic terminology and risks related to the relevant business sector practices. 审查审核报告并做出认证决定的人员应具备以下方面的知识： a) 与相关业务领域实践相关的通用术语和风险。	Experience in management system certification, 2 Years as Lead Auditor for an ISO 17021-1 related standard or 2 years of full time employment for a ISO 27001 accredited CB 应具备管理体系认证经验，担任与 ISO 17021 - 1 相关标准的审核组长 2 年，或在获得 ISO 27001 认可的认证机构全职工作 2 年
7.1.2.4.5 Client products, processes and organization 客户的产品、流程和组织架构 Personnel reviewing audit reports and making certification decisions shall have knowledge of: a) client products, processes, organization types, size, governance, structure, functions and relationships. 审查审核报告并做出认证决定的人员应具备以下方面的知识： a) 客户的产品、流程、组织类型、规模、管理模式、架构、职能以及相互关系。	Experience in Information Management Systems, as required for Auditors (min. level Observer) 需具备信息管理体系方面的经验，达到审核员所要求的水平（最低为观察员级别）

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com