华测认证

隐私信息管理体系认证规则

文 件 编 号：CTI-PIMS-2021

文 件 版 本： A/02

生 效 日 期： 2025-08-15

批 准 人：

华测认证有限公司

CTI Certification Co., Ltd.

序号	文件状态		创建日期	编制人	审核人	批 准
0	A/00		2021-11-20	杜江 王群	孙健	王珺
序号	**修订章节**	**修订内容摘要**	**修订状态**	**修订日期**	**修订人**	**审核人**	**批 准**
1	……	依据认监委公告2025年第9号文件进行全面修改同时简化附录A审核时间计算方法。	A/01	2025-05-30	古跃东 宋鹏	孙健	周璐
2	第4、7、8章	1. 明确审核方案、证书恢复、变更等要求及认证证书管理要求； 2. 勘误	A/02	2025-08-15	古跃东	孙健	周璐

目 录

1 目的、适用范围及认证依据

1.1本规则用于规范华测认证有限公司（以下简称：CTI）依据 ISO/IEC27701《安全技术 基于 ISO/IEC 27001 和 ISO/IEC 27002 对隐私信息管理的扩展 要求和指南》标准开展的隐私信息管理体系（PIMS）认证活动。

1.2认证依据：ISO/IEC27701《安全技术 基于 ISO/IEC 27001 和 ISO/IEC 27002 对隐私信息管理的扩展 要求和指南》

1.3本规则依据认证认可相关法律法规，结合相关技术标准，对隐私信息管理体系认证实施过程作出具体规定，明确 CTI 对隐私信息管理体系认证过程的管理责任，保证隐私信息管理体系认证认证活动的规范有效。

2 华测认证的基本要求

2.1CTI 按照 CNAS-CC170《信息安全管理体系认证机构要求》、CNAS-SC170《信息安全管理体系认证机构认可方案》、ISO/IEC27701：2019《安全技术 基于 ISO/IEC 27001 和 ISO/IEC 27002 对隐私信息管理的扩展 要求和指南》认证所涉及的认证能力、内部管理和工作过程。

2.2CTI 建立内部制约、监督和责任机制，实现培训（包括相关增值服务）、审核和作出认证决定等工作环节相互分开，以符合公正性要求。

2.3CTI 提供的隐私信息管理体系认证可结合其他管理体系认证活动进行。

3 对认证人员的基本要求

3.1认证审核人员应当取得中国认证认可协会（CCAA）的信息安全管理体系注册审核员资格，并经过隐私信息管理体系相关标准的培训并评价合格。专业审核人员应具有相应行业的专业背景并经评价满足相应专业能力。

3.2其他人员（如认证规则和认证方案制定人员、申请评审人员、方案管理人员、认证决定人员、能力评价人员等）， 应经评价确认满足 CTI 确定的能力要求。

3.3认证人员应当遵守与从业相关的法律法规，对认证审核活动及相关认证审核记录和认证审核报告的真实性承担相应的法律责任。

4 初次认证程序

4.1受理认证申请

4.1.1 认证申请组织应具备以下条件：

（1）取得国家工商行政管理部门或有关机构注册登记的法人资格或其组成部分；

（2）已取得相关法规规定的行政许可（适用时）；

（3）认证范围涉及的产品或提供的服务符合国家相关法律、法规和有关规范的要求；

（4）隐私信息管理体系（PIMS）是在 ISO/IEC 27001 信息安全管理体系的基础上建立、实施和扩展的，ISMS 是 PIMS 的基础和前提条件。申请 PIMS 的组织应已经建立信息安全管理体系，且通过了 ISMS 认证或准备同时申请 ISMS 认证。并建立和实施了企业隐私信息管理体系，且有效运行 3 个月以上；

（5）在一年内，未发生违反国家相关法律法规的事故；

（6）三年内未因违反相关法律法规而被其他认证机构撤销隐私信息管理体系认证证书；

（7）未被执法部门责令停业整顿或在全国企业信用公示系统中被列入“严重违法企业名单”。

4.1.2 认证申请组织应提交的文件和资料：

（1） 认证申请书；

（2） 有效的 ISMS 认证证书或 ISMS 认证申请；

（3） 法律地位的证明文件的复印件。若隐私信息管理体系覆盖多场所活动，应附每个场所的法律地位证明文件的复印件（适用时）；

（4） 隐私信息管理体系覆盖的活动所涉及法律法规要求的行政许可证明、资质证书、强制性认证证书等的复印件 ；

（5） 个人可识别信息（PII）识别处理 PII 信息流涉及的信息系统、存储介质等清单

（6） PII 风险评估报告

（7） PII 影响分析报告

（8） 公司场景与角色识别表

（9） 适用性声明；

（10）适用的法律法规清单

（11）其他需要的文件。

组织的 ISMS 发证机构非 CTi 时，除上述规定需提交的资料外，还需同步提交组织 ISMS 的申请资料：

1） 信息安全管理体系方针和目标；

2） 支持信息安全管理体系的规程和控制措施；

3） 信息安全风险评估报告（含风险评估方法的描述）；

4） 信息安全残余风险报告；

5） 信息安全风险处置计划；

6） 信息安全管理体系适用性声明；

7）信息安全管理体系适用的法律法规的标准的清单；

4.1.3 申请评审

CTI 对申请认证组织提交的申请资料进行评审，根据申请认证的活动范围及场所、员工人数、完成认证活动所需时间和其他影响认证活动的因素，综合确定是否受理认证申请。

4.1.4 评审结果处理

申请材料齐全并符合有关要求的，予以受理认证申请。未通过申请评审的，CTI 书面通知申请组织在规定时间内补充和完善，或不受理认证申请并明示理由。

4.1.5 签订认证合同

在实施认证审核之前，CTI 与认证申请组织订立具有法律效力的书面认证合同，明确拟认证的范围，以及在认证审核实施过程及认证证书有效期内，认证机构和申请组织各自应当承担的责任、权利和义务。

4.2审核方案和审核策划

4.2.1 审核方案

4.2.1.1 CTI 应针对每一认证组织建立认证周期内的审核方案，以清晰地识别所需的审核活动。

4.2.1.2 初次认证的审核方案应包括两阶段初次审核、获证后的监督审核和认证到期前进行的再认证审核。

注：一个认证周期通常为 3 年，从初次认证（或再认证）决定算起，至认证的有效期截止。

4.2.1.3 初次认证审核和再认证审核是对认证组织完整体系的审核，应覆盖 ISO/IEC27701 所有要求，以及认证范围内的典型隐私信息安全。认证证书有效期内的监督审核应覆盖 ISO/IEC27701 所有要求。

4.2.1.4 初次认证及再认证后的第一次监督审核应在证书签发起 12 个月内进行。此后，监督审核应至少每个日历年（应进行再认证的年份除外）进行一次，且两次监督审核的时间间隔不得超过 15 个月。

4.2.1.5 CTI 应考虑认证组织不同班次完成的过程，以及其所证实的对每个班次的隐私信息管理体系控制水平来策划对不同班次实施的审核程度，以确保审核的有效性：

（1）每次审核应至少对其中的一个班次的生产或服务的活动现场进行审核；

（2）对于未审核的班次，应记录不对其审核的理由。

4.2.1.6 对于多场所组织，当组织活动、过程相同或高度相似时可进行抽样，抽样数量如

下：

（1）初次认证审核：样本的数量应为场所数量的平方根（Y=$\sqrt{x}$ ），计算结果向上取整为最接近的整数，其中 y 为将抽取场所的数量、x 为场所总数。

（2）监督审核： 每年的抽样数量应为场所数量的平方根乘以 0.6 即（y＝0.6 $\sqrt{x}$），计算结果向上取整为最接近的整数。

（3）再认证审核：样本的数量应与初次审核相同。然而，如果证明管理体系在认证周期中是有效的，样本的数量可以减少至乘以系数 0.8 即（y＝0.8 $\sqrt{x}$），计算结果向上取整为最接近的整数。

中心职能在初次审核、证书有效期的每次监督审核、再认证审核都应接受审核。

对于不满足抽样条件的多场所组织，审核方案的构成应包括对所有场所的初次认证审核和再认证审核。在监督审核中，应在每个日历年覆盖 30%的场所（向上取整至整数）。每次审核都包括中心职能。第二次监督审核选取的场所通常不同于第一次监督审核所选取的场所。

4.2.2 审核时间

CTI 根据管理体系认证审核时间的相关要求，确定隐私信息管理体系认证审核所需的时间，以确保审核的充分性和有效性。隐私信息管理体系初次认证审核的审核时间按照 附录 A 隐私信息管理体系认证审核时间要求。

4.2.3 审核组

CTI 根据隐私信息管理体系认证覆盖的活动的专业技术领域选择具备相关能力的审核员组成审核组，必要时选择技术专家参加审核组。审核组中的审核员承担审核任务和责任。

技术专家主要负责提供认证审核的技术支持，不作为审核员实施审核，不计入审核时间，其在审核过程中的活动由审核组中的审核员承担责任。

4.2.4 审核计划

4.2.4.1 审核组长为每次审核制定书面的审核计划。审核计划至少包括以下内容：审核目的、审核准则、审核范围、现场审核的日期和场所、现场审核持续时间、审核组成员（其中：审核员应标明认证人员注册号；技术专家应标明专业代码、工作单位及专业技术职称）。

4.2.4.2 若隐私信息管理体系覆盖范围包括多个场所进行相同或相近的活动，且这些场所都处于申请组织的授权和控制下，可以根据 CTI 多现场组织审核抽样的有关要求，在审核中对这些场所进行抽样。如果不同场所的活动存在明显差异、或不同场所间存在可能对隐私信息管理有显著影响的区域性因素，则不能采用抽样审核的方法，应当逐一到各现场进行审核。

4.2.4.3 为使现场审核活动能够观察到相关过程的隐私信息管理情况，现场审核将安排在认证范围覆盖的活动正常运行时进行。

4.2.4.4 在审核活动开始前，审核组长应将审核计划提交申请组织确认，遇特殊情况临时变更计划时，应及时将变更情况通知申请组织，并协商一致。

4.3实施审核

4.3.1 审核组应当按照审核计划的安排完成审核工作。除不可预见的特殊情况外，审核过程中不得更换审核计划确定的审核员。

4.3.2 审核组应当会同申请组织按照程序顺序召开首、末次会议，申请组织的最高管理者及与隐私信息管理体系相关的职能部门负责人员应该参加会议。参会人员应签到，审核组应当保留首、末次会议签到表。申请组织要求时，审核组成员应向申请组织出示身份证明文件。

4.3.3 审核过程及环节

4.3.3.1 初次认证审核，分为第一、二阶段实施审核。

4.3.3.2 第一阶段审核应至少覆盖以下内容：

（1）结合现场情况，确认申请组织实际情况与隐私信息管理体系成文信息描述的一致性，特别是体系成文信息中描述的产品和服务、部门设置和职责与权限、生产或服务过程等是否与申请组织的实际情况相一致。

（2）结合现场情况，审核申请组织理解和实施 ISO/IEC27701：2019 标准要求的情况，评价隐私信息管理体系运行过程中是否实施了内部审核与管理评审，确认隐私信息管理体系是否已运行并且超过 3 个月。

（3）确认申请组织建立的隐私信息管理体系覆盖的活动内容和范围、体系覆盖范围内有效人数、过程和场所，遵守适用的法律法规及强制性标准的情况。

（4）结合隐私信息管理体系覆盖产品和服务的特点识别对隐私信息管理风险和隐私信息

管理目标实现具有重要影响的关键点，并结合其他因素，科学确定重要审核点。

（5）与申请组织讨论确定第二阶段审核安排。对隐私信息管理体系成文信息不符合现场实际、相关体系运行尚未超过 3 个月或者无法证明超过 3 个月的，以及其他不具备二阶段审核条件的，不应实施二阶段审核。

4.3.3.3 在下列情况，第一阶段审核可以不在申请组织现场进行，但应记录未在现场进行的原因：

（1）申请组织已获 CTI 颁发的其他有效认证证书，CTI 已对申请组织隐私信息管理体系有充分了解。

（2）CTI 有充足的理由证明申请组织的生产经营或服务过程的隐私信息管理活动清晰、隐私信息管理风险小，通过对其提交文件和资料的审查可以达到第一阶段审核的目的和要求。

除以上情况之外，第一阶段审核应在受审核方的生产经营或服务现场进行。

4.3.3.4 审核组应将第一阶段审核情况形成书面文件告知申请组织。对在第二阶段审核中可能被判定为不符合项的重要关键点，要及时提醒申请组织特别关注。

4.3.3.5 第二阶段审核应当在申请组织现场进行。重点是审核隐私信息管理体系符合 ISO/IEC27701：2019 标准要求和有效运行情况，应至少覆盖以下内容：

（1）在第一阶段审核中识别的重要审核点的产品和服务的隐私信息必需的过程控制措施的有效性。

（2）为实现隐私信息管理方针而在相关部门、层次和过程上建立隐私信息管理目标是否具体适用、可测量并得到沟通、监视。

（3）对 PII 识别处理 PII 信息流涉及的信息系统、存储介质等、PII 风险评估、PII 影响分析、满足隐私信息管理范围内的产品和服务必需过程的运行策划和控制、隐私信息管理绩效评价的管理及控制情况。

（4）申请组织实际工作记录是否真实。对于审核发现的真实性存疑的证据应予以记录并在做出审核结论及认证决定时予以考虑。

（5）申请组织的 PII 识别处理 PII 信息流涉及的信息系统、存储介质等、PII 风险评估、PII 影响分析、内部审核和管理评审是否有效。

4.3.4 发生以下情况时，审核组应向认证机构报告，经认证机构同意后终止审核。

（1）受审核方对审核活动不予配合，审核活动无法进行。

（2）受审核方实际情况与申请材料有重大不一致。

（3）其他导致审核程序无法完成的情况。

4.4审核报告

4.4.1 审核组根据审核的结果，形成书面审核报告。审核报告描述审核活动的主要内容，包括：

（1）申请组织的名称和地址；

（2）申请组织活动范围和场所；

（3）审核的类型、准则和目的；

（4）审核组组长、审核组成员及其个人注册信息；

（5）审核活动的实施日期和地点，包括固定现场和临时现场；对偏离审核计划情况的说明，包括对审核风险及影响审核结论的不确定性的客观陈述；

（6）叙述从 4.3 条列明的程序及各项要求的审核工作情况，其中对 4.3.3.5 条的各项审核要求应逐项描述或引用审核证据、审核发现和审核结论；对隐私信息管理目标和过程及隐私信息管理绩效实验情况进行评价。

（7）识别出的不符合项；

（8）审核组对是否通过认证的意见建议。

4.4.2 CTI 保留用于证实审核报告中相关信息的证据。

4.4.3 CTI 应在作出认证决定后 30 个工作日内将审核报告提交申请组织。

4.4.4 对终止审核的项目，审核组应将已开展的工作情况形成报告，CTI 应将此报告及终止审核的原因提交给申请组织，并保留签收或提交的证据。

4.5不符合项的纠正和纠正措施及其结果的验证

对于审核中发现的不符合，审核组将出具书面不符合报告。CTI 将要求申请组织分析原因，并提出纠正和纠正措施。对于严重不符合，将要求申请组织在最多不超过 6 个月期限内采取纠正和纠正措施。CTI 将对申请组织所采取的纠正和纠正措施及其结果的有效性进行验证。如果未能在第二阶段结束后 6 个月内验证对一般不符合或严重不符合实施的纠正和纠正措施，则应按 4.6.5 条处理，或者按照 4.3.3.5 条重新实施第二阶段审核。

4.6认证决定

4.6.1 CTI 在对审核报告、不符合项的纠正和纠正措施及验证情况和其他信息进行复核、综合评价的基础上，做出认证决定。

4.6.2 认证决定人员应为 CTI 管理控制下的人员，审核组成员不得参与对审核项目的认证决定。

4.6.3 CTI 在作出认证决定前应确认如下情形：

（1）审核报告符合本规则第 4.4 条要求，审核组提供的审核报告及其他信息能够满足作出认证决定所需要的信息。

（2）反映以下问题的不符合项，CTI 已评审、接受并验证了纠正和纠正措施的有效性。

①在持续改进隐私信息管理体系的有效性方面存在缺陷，实现隐私信息管理目标有重大疑问。

②制定的隐私信息管理目标不可测量、或测量方法不明确。

③对实现隐私信息管理目标具有重要影响的关键点的监视和测量未有效运行，或者对这些关键点的报告或评审记录不完整或无效。

④其他严重不符合项。

（3）CTI 对其他一般不符合项已评审，并接受了申请组织计划采取的纠正和纠正措施。

4.6.4 在满足 4.6.3 条要求的基础上，CTI 有充分的客观证据证明申请组织满足下列要求的，可评定该申请组织符合隐私信息管理体系认证要求，向其颁发隐私信息管理体系认证证书：

（1）申请组织的隐私信息管理体系符合认证依据的要求且运行有效。

（2）认证范围覆盖的产品和服务符合相关法律法规要求。

（3）申请组织按照认证合同规定履行了相关义务。

4.6.5 当申请组织不能满足上述要求的，则评定该申请组织不符合隐私信息管理体系认证要求，CTI 将以书面形式告知申请组织并说明其未通过认证的原因。

5 监督审核

5.1CTI 将对颁发的隐私信息管理体系认证证书的组织（以下称获证组织）进行有效跟踪，监督获证组织持续运行隐私信息管理体系并符合认证要求。

5.2作为最低要求，初次认证后的第一次监督审核应在认证证书签发日起 12 个月内进行，两次监督审核的间隔不超过 15 个月，当获证组织的隐私信息管理体系发生重大变更，或企业发生重大失信行为时，CTI 将增加跟踪监督的频次。

5.3超过期限而未能实施监督审核的，应按 7.1 或 7.2 条处理。

5.4监督审核的时间应不少于初次认证审核人日数的 1/3。

5.5监督审核的审核组应满足 4.2.2 要求。

5.6监督审核应在获证组织现场进行，应满足 4.2.3.3 要求。

5.7监督审核时至少覆盖以下内容：

（1）上次审核以来隐私信息管理体系覆盖的活动及影响体系的重要变更及运行体系的资源是否有变更。

（2）按 4.3.3.2（4）条要求已识别的重要关键点是否按隐私信息管理体系的要求在正常和有效运行。

（3）对上次审核中确定的不符合采取的纠正和纠正措施是否继续有效；

（4）隐私信息管理目标及隐私信息管理绩效是否达到预期，如果没有达到，获证组织是否识别了原因、确定并实施了改进措施；

（5）组织企业隐私信息管理体系覆盖的活动所涉及法律法规的持续符合性；

（6）内部审核和管理评审是否规范和有效；

（7）是否及时接受和处理投诉；

（8）认证证书和标志的使用以及对认证资格的引用；

（9）针对体系运行中发现的问题或投诉，及时制定并实施了有效的改进措施。

5.8对于监督审核中发现的不符合，获证组织应在规定时限内完成纠正和纠正措施并提供纠正和纠正措施有效性的证据。CTI 将对获证组织所采取的纠正和纠正措施及其结果的有效性进行验证。

5.9监督审核的审核报告按照 5.7 条列明的审核要求逐项描述或引用审核证据、审核发现和审核结论。CTI 将根据监督审核报告及其他相关信息，作出继续保持或暂停、撤销认证证书的决定。

6 再认证程序

6.1隐私信息管理体系认证证书有效期满前三个月，获证组织可向 CTI 提出再认证申请。

6.2隐私信息管理体系再认证程序与初次认证程序一致。在获证组织的隐私信息管理体系及获证组织的内部和外部环境、PII 识别处理 PII 信息流涉及的信息系统、存储介质等、PII 风险评估、PII 影响分析等无重大变更时，再认证审核可省略第一阶段审核。

6.3隐私信息管理体系再认证审核的时间不少于初次认证审核人日数的 2/3。

6.4对于再认证审核中发现的不符合，获证组织应在规定时限内完成纠正和纠正措施并提供纠正和纠正措施有效性的证据。CTI 将对获证组织所采取的纠正和纠正措施及其结果的有效性进行验证。

6.5CTI 按照 4.6 的要求作出再认证决定。获证组织继续满足认证要求并履行认证合同义务的，向其换发认证证书。

6.6如果在当前认证证书的终止日期前完成了再认证活动并决定换发证证书，新认证证书的终止日期可以基于当前认证证书的终止日期。新认证证书上的颁证日期应不早于再认证

决定日期。

如果在当前认证证书终止日期前，CTI 未能完成再认证审核或对严重不符合项实施的纠正和纠正措施未能进行验证，则不应予以再认证，也不应延长原认证证书的有效期。

在当前认证证书到期后，如果 CTI 能够在 6 个月内完成未尽的再认证活动，则可以恢复认证，否则应至少进行一次第二阶段审核才能恢复认证。认证证书的生效日期应不早于再认证决定日期，终止日期应基于上一个认证周期。

7 认证资格的暂停或恢复，撤销，注销和扩大或缩小认证范围

7.1暂停证书

获证组织有下列情形之一的，CTI 将暂停其使用隐私信息管理体系认证证书，暂停期限最长为六个月：

（1）隐私信息管理体系持续或严重不满足认证要求；

（2）不承担、履行认证合同约定的责任和义务

（3）被有关执法监管部门责令停业整顿；

（4）发生隐私信息泄漏事故，或受到相关方关于隐私信息的重大投诉，但尚不需立即撤销认证证书；

（5）未能按规定间隔期接受监督审核；

（6）主动申请暂停认证证书；

（7）其他应当暂停认证证书的。

7.2撤销证书

获证组织有下列情形之一的，CTI 将撤销其隐私信息管理体系认证证书：

（1）被注销或撤销法律地位证明文件或有关的行政许可证明和资质证书；

（2）被国家市场监督管理总局列入信用严重失信企业名单；

（3）拒绝配合 CTI 或认证监管部门实施的监督检查，或者对有关事项的询问和调查提供了虚假材料或信息的；

（4）出现重大事故，经执法监管部门确认是获证组织违规造成；

（5）有其他严重违反法律法规行为的；

（6）暂停认证证书的期限已满但导致暂停的问题未得到解决或纠正的；

（7）没有运行隐私信息管理体系或者已不具备运行条件的；

（8）不按相关规定正确引用和宣传获得的认证信息，造成严重影响或后果，或者认证机构已要求其纠正但超过 2 个月仍未纠正的；

（9）主动申请撤销认证证书的；

（10）其他应当撤销认证证书的。

7.3注销证书

获证组织主动申请不再保持认证证书时，CTI 应确认在不存在暂停或撤销情形后，注销其认证证书，并保留相应证据。

7.4CTI 将以书面方式通知获证组织有关暂停、撤销或注销隐私信息管理体系认证证书的信息和要求，并在 CTI 网站上公布相关信息，同时按规定程序和要求上报国家认监委。对于撤销或注销认证证书的，CTI 将收回撤销或注销的隐私信息管理体系认证证书。

7.5被暂停、撤销或注销隐私信息管理体系认证证书的获证组织，不得以任何方式使用认证证书、认证标识或引用认证信息。

7.6 暂停证书的恢复

获证组织接到暂停证书通知后，在规定时间内对证书暂停原因采取了纠正和纠正措施，经 CTI 验证，造成暂停的原因已消除的，CTI 将恢复其认证注册资格，并在 CTI 网站上公布相关信息，同时按规定程序和要求上报国家认监委。

7.7扩大或缩小认证范围

（1）获证组织需扩大认证范围时应提出申请，CTI 将评审申请，确定必要的审核活动，以做出是否可予扩大的决定。

（2）如果认证范围的某些部分（如产品、区域）持续或严重地不满足认证要求，会导致认证范围的缩小。获证组织范围内某些部分不愿维持纳入认证资格，也可提出缩小认证范围。

（3）认证范围扩大或缩小后，CTI 将换发变更后的认证证书，同时将相关信息上报国家认监委。

8 认证证书及认证标志

8.1隐私信息管理体系认证证书至少包含以下信息：

（1）获证组织名称、地址和统一社会信用代码；

（2）认证覆盖的生产/经营或服务的地址和业务范围；

（3）认证依据的标准、技术要求；

（4）证书编号；

（5）证书颁证日期、证书有效期；

（6）CTI 名称、地址和认证标志；

（7）证书查询方式；

（8）其他需说明的内容。

8.2 隐私信息管理体系认证证书有效期为 3 年，再认证的认证证书有效期不超过最近一次有效认证证书截止期再加 3 年。

8.3 CTI 按照认监委相关信息通报制度上报隐私信息管理体系认证证书信息。

8.4 认证证书与认证标志使用要求：按《管理体系认证标志、认可标识和认证状态声明管理规定》。

9 与其他管理体系的结合审核

9.1当隐私信息管理体系认证审核和其他管理体系认证审核结合实施时，应同时遵照本规则要求以及其他管理体系认证的相关要求。

9.2结合审核的审核时间人日数，不得少于多个单独体系所需审核时间之和的 80%。

10 申诉和投诉

10.1 申请组织或获证组织对认证决定有异议时，可向 CTI 提出申诉。CTI 自收到申诉之日起，在 60 日内进行处理，并将处理结果书面通知申诉人。

10.2 书面通知应当告知申诉人，若认为 CTI 未遵守认证相关法律法规或本规则并导致自身合法权益受到严重侵害的，可以直接向所在地认证监管部门或国家认监委投诉，也可以向相关认可机构投诉。

11 收费

收费由 CTI 按照有关规定收取，认证委托方应按时、足额缴纳认证费用。

附录 A　隐私信息管理体系认证审核时间要求

A.1 确定基础审核时间准则

基于本标准是信息安全管理体系标准要求针对个人信息安全管理体系措施扩展控制集，确定本标准的审核时间，将根据同等条件下，组织信息安全管理体系确定的审核时间，乘以本标准所增加的控制措施数量与信息安全管理体系附录 A 控制控制措施条款的数量之比，即：

本标准审核时间 = K * ISMS 审核时间

K=本标准控制措施数量 / 信息安全管理体系控制措施数量 = 86/114≈0.8　（保留小数点一位 ）

注 1：本标准控制措施数量计算：ISO/IEC27701:2019 共修订了 37 个控制条款， 增加了 49 个 PIMS 特定的控制条款（控制者 31 个控制条款、处理者 18 个控制条款）。本标准控制条款数量最终等效于 86 个控制措施条款。

注 2：ISMS 审核时间如下；

在组织控制下工作的人员的数量	初审（第一阶段+第二阶段）审核时间（天）	在组织控制下工作的人员的数量	初审（第一阶段+第二阶段）审核时间（天）
1 ~ 10	5	876 ~ 1175	18.5
11 ~ 15	6	1176 ~ 1550	19.5
16 ~ 25	7	1551 ~ 2025	21
26 ~ 45	8.5	2026 ~ 2675	22
46 ~ 65	10	2676 ~ 3450	23
66 ~ 85	11	3451 ~ 4350	24
86 ~ 125	12	4351 ~ 5450	25
126 ~ 175	13	5451 ~ 6800	26
176 ~ 275	14	6801 ~ 8500	27
276 ~ 425	15	8501 ~ 10700	28
426 ~ 625	16.5	＞ 10700	沿用以上规律
626 ~ 875	17.5		

A.2 审核时间调整因素

在本标准 PIMS 领域审核时间的确定后，可以根据申请组织的实际情况，按照规定进行调整，除此之外还可以考虑以下因素：

A.2.1　增加审核时间的考虑因素：

1)　信息安全管理体系的确认增加 0.5 人日

由于组织申请认证本标准已经建立并运行信息安全管理体系标准并通过认证审核,或与本标准同时申请认证审核。因此在采信组织信息安全管理体系认证结果时，同样要针对原信息安全管理体系运行进行确认审核 确认的内容包含但不限于：

a)　本标准的管理方针与目标是否建立与实施

b） 本标准所涉及到的相关责任是否已得到分配

c） 信息安全管理体系内审与管评是否包含了本标准的要求；

d） 关键场所、系统、信息的保护措施是否有效。

注 3： 该项调整因素不进行 70%的折算，即直接加在现场审核人日中。

2) CTI 已经颁发了 ISMS 认证证书，拟安排同一审核组长，但是据上次审核已经超过 180 天。应增加审核时间 5%-10%；

3) 申请组织取得其他 ISMS 机构的认证证书，据上次审核时间小于 180 天时。应增加 5%-10%；

4) 申请组织取得其他 ISMS 机构的认证证书，据上次审核时间超过 180 天时。应增加 15%-20%；

A.2.2 减少审核时间的考虑因素

对于 CTI 颁发的 ISMS 认证证书，最近一次 ISMS 审核日期与 PIMS 审核日期小于 180 天，且 ISMS 和 PIMS 审核组长为同一人时，可以减少 10%；

按照上述要求基础审核时间进行调整后得到项目最终的审核时间，其审核时间包含现场审核和非现场审核时间。

A.3 现场审核人日

现场审核人日不得小于 70%的审核时间。

注 1：PIMS 是基于 ISMS 扩展的管理体系，PIMS 扩展的要求有两个方面：一是在原有的 ISMS 相应的条款延展了隐私管理的范围，ISMS 标准正文中延展了 20%的要求；ISMS 标准的附录 A 中延展了 50%要求；二是在 ISMS 标准附录 A 中的 114 个控制条款基础上，；另外还要考虑附录 A 的控制条款是被重复审核的情况。

附录 B　认证业务范围分类

大类	中类	风险等级	类别说明	对应ISMS专业类别
01政务	01.01	低	其他	01.04
	01.02	高	国家机构/税务机关/海关	01.01/01.02/01.03
02公共	02.01	低	科研/社会保障/医疗服务/教育/其他	02.03/02.04/02.05/02.06/02.07
	02.02	高	通信、广播电视/新闻出版	02.01/02.02
03商务	03.01	低	咨询中介/旅游、宾馆、饭店/其他	03.04/03.05/03.06
	03.02	高	金融/电子商务/物流	03.01/03.02/03.03
04产品的生产	04.01	低	交通运输/信息与通信技术/冶金/采矿/食品、药品、烟草/农、林、牧、副、渔业/其他	04.07/04.08/04.09/04.10/04.11/04.12/04.13
	04.02	高	电力/铁路/民航/化工/航空航天/水利	04.01/04.02/04.03/04.04/04.05/04.06

PIMS 是 ISMS 的扩展，业务范围管理基于 ISMS 的划分实施，并基于 PIMS 的特点进行了合并。