华亿认证中心
HUAYI CERTIFICATION CENTER

管理体系认证规则（二十二）

HYC-MSCR-022-2023

编 制	审 核	批 准	版本号	
编制小组	评审组	焦大川	A/0	
修订说明		修订页数	修订日期	批 准

发布日期：2023 年 11 月 20 日　　实施日期：2023 年 11 月 20 日

华亿认证中心有限公司　发布

目　录

1. 目的

为规范个人身份信息保护管理体系认证实施规则认证工作，保证认证的规范性和有效性，根据《中华人民共和国认证认可条例》、《认证机构管理办法》和《国家认监委关于认证规则备案的公告》等认证认可相关法律法规和规章的要求，制订本规则。

2. 适用范围

本规则依据《中华人民共和国认证认可条例》、《认证机构管理办法》等认证认可相关法律法规，结合相关技术标准，规定了本机构开展个人身份信息保护管理体系认证实施规则认证活动应遵循的基本程序要求。除国家认监委另有规定外，本机构在中国境内从事个人身份信息保护管理体系认证实施规则认证活动应当遵守本规则要求。

3. 依据标准

个人身份信息保护管理体系认证实施规则认证依据标准：ISO/IEC 29151:2017《信息技术 安全技术 个人身份信息保护实践指南》。

4. 对认证机构的基本要求

4.1 华亿认证应当依据认证认可相关法律法规取得认证相关资质后，方可在批准范围内开展相关个人身份信息保护管理体系认证实施规则认证活动。

4.2 华亿认证从事认证活动应当遵循公正公开、客观独立、诚实信用的原则。华亿认证实施内部管理和开展认证活动应当符合GB/T 27021.1《合格评定 管理体系审核认证机构要求 第1部分：要求》及其他相关系列标准要求，以确保持续具备开展个人身份信息保护管理体系认证实施规则认证的能力、一致性和公正性。

4.3 华亿认证开展个人身份信息保护管理体系认证实施规则认证活动，应根据国家经济和社会发展的需要，不得影响国家安全和社会公共利益，不得违背社会公

序良俗。

4.4 华亿认证开展不同类别、不同行业领域的个人身份信息保护管理体系认证实施规则认证活动，应当在遵守本规则基础上，制定机构自身的认证实施规则（如认证方案、认证程序、作业指导书等），并遵照执行。

4.5 华亿认证应当建立风险防范机制，对其从事个人身份信息保护管理体系认证实施规则认证活动可能引发的风险和责任，采取合理有效措施。华亿认证应能证明已对其开展的管理体系认证活动引发的风险进行了评估，并对各个活动领域和运作地域的业务引发的责任做充分安排（如保险或储备金）。

获证组织发生重大事故或引发重大舆情，华亿认证应及时采取措施，迅速进行调查、处理，应当在得知信息2日之内报送市场监管政府主管部门。

4.6 华亿认证应当建立认证人员管理制度，对认证人员的选择条件、评价准则、聘用程序、培养机制等做出明确规定，确保从事不同类型、不同行业领域个人身份信息保护管理体系认证实施规则认证的人员持续具备相应素质和能力。其中，下列三类人员，其能力应当满足GB/T27021（或ISO/IEC 17021）系列标准中的相应要求：

（1）实施申请评审以确定所需的审核组能力要求，选择审核组成员，并确定审核时间；

（2）复核审核报告并作出认证决定；

（3）审核及领导审核组。

4.7 华亿认证应当基于风险思维，对不同类型的获证组织开展有效的监督活动，以监督获证组织持续运行个人身份信息保护管理体系认证实施规则并符合认证要求。除了常规的监督审核以外，华亿认证还应根据获证组织的环境复杂程度，开展多种形式的监督活动，包括：

（1）审核组织对其运作的说明（如宣传材料、网页）；

（2）就认证的有关方面询问组织或要求提供文件化信息；

（3）跟踪行政监管部门发布的监管信息；

（4）跟踪媒体发布的信息；

（5）特殊审核，如提前较短时间通知的突击检查；

（6）其他监视获证组织绩效的方法，如互联网、大数据技术等。

5. 对认证人员的基本要求

5.1 华亿认证从事个人身份信息保护管理体系认证实施规则认证审核的人员应当为：

（1）取得中国认证认可协会（CCAA）的信息安全管理体系（ISMS）注册审核员资格，应符合国家认证人员职业资格的相关要求。

（2）专业认证人员应具有相应行业的专业能力。

（3）经过相关标准的培训，并应满足从事相应认证活动所需的相关知识与技能要求。

5.2 认证人员应遵守认证认可相关法律法规及规范性文件的要求，应当具有从事认证工作的基本职业操守：诚信、客观、公正、廉洁，不冒名顶替其他认证人员实施审核，不编制虚假或严重失实的文件，不出具虚假或严重失实的认证记录和报告，不编造学习经历、工作经历和审核经历。认证人员对认证结论、认证结果的真实性承担相应责任。

5.3 认证人员应当具备与其所从事认证工作相适宜的能力，且为保证自身能力持续满足认证相关要求，应当持续学习，并定期参加华亿认证组织或要求的各类培训。

5.4 认证人员不得发生影响认证公正性和有效性的行为；不得参与近两年内其咨

询过的组织的认证活动；不得接受认证委托人及其相关利益方的礼金、礼品或其他不当利益；未经允许不得私自到获证组织报销食宿交通等票据。

6. 认证申请

6.1 信息公开

华亿认证应当向申请组织至少公开以下信息：

（1）可开展认证服务的范围，以及获得认可的情况；

（2）开展认证活动所依据的认证标准及认证流程；

（3）相关的认证方案、认证程序；

（4）授予、拒绝、保持、更新、暂停（恢复）或撤销认证以及扩大或缩小认证范围的程序规定；

（5）拟向组织获取的信息，以及对相关信息的保密规定；

（6）认证证书、认证标志及相关的使用规定；

（7）对认证过程的申诉、投诉规定；

（8）认证依据用标准转版的规定；

（9）公正性政策。

6.2 申请信息

华亿认证应当要求认证申请组织提供必要的信息，至少包括：

（1）申请的认证范围；

（2）申请认证依据的标准或其他要求；

（3）法律地位的证明性文件。覆盖多个法律实体时，应提供每个场所的法律地位证明性文件；

（4）申请认证范围所涉及的法律法规要求的行政许可证明、资质证书、强制性认证证书等资质文件；

（5）申请组织的名称、地址、组织机构及其他与管理体系运行相关的详细信息，包括影响体系有效性的外包过程；

（6）相关资质证明文件（如：其他管理体系认证证书）；

（7）管理体系文件；

（8）受审核方实施了内部审核与管理评审的相关证据；

（9）其他与申请PIIPMS认证相关的材料。

6.3 申请评审

6.3.1 华亿认证应当实施认证申请评审，以确定是否受理认证申请，不得受理本机构未被批准或不具备专业能力的认证申请。

6.3.2 存在以下情况的组织，华亿认证不得受理其认证申请：

（1）申请组织的认证申请范围与其实际经营范围明显不符，且不愿意协商的；

（2）被全国企业信用信息公示系统或者政府其他信用公示系统列入严重违法失信名单的；

（3）申请组织被行政执法部门或其他部门责令停业整顿，或因发生重大环境污染、安全事故、供应链中断、被行政处罚并在行政处罚执行期的；

（4）申请组织的规模、人数或经营状况明显不适用体系运行的；

（5）申请组织涉及国家安全、政治组织、社会民俗、民族宗教等领域，在国家认监委统筹安排前的；

（6）其他违反国家法律法规、行业规定的情形。

6.4 认证合同

6.4.1 华亿认证应当与每个申请组织订立具有法律效力的认证合同或等效文件，以明确双方的责任。

6.4.2 华亿认证的责任至少包括：

（1）及时向符合认证要求的客户颁发认证证书，并经获证组织同意后，通过相应媒体公布获证信息；

（2）因华亿认证原因（如机构被注销或撤销），导致客户证书无法有效保持的，需及时告知客户并作出妥善处理。

6.4.3 申请组织的责任至少包括：

（1）遵守认证要求，如实提供相关材料和信息并协助市场监管和知识产权管理部门的监督检查。

（2）获证后，正确使用认证证书和认证标志。包括在其认证证书被暂停、撤销后，立即停止使用认证证书和所有引用认证资格的广告材料。

（3）发生如下情况，及时向华亿认证通报：发生重大变更、被政府主管部门公布检查不合格、被媒体曝光存在问题、受到相关行政处罚、发生重大事故、管理体系不能正常运行或发生重大变化等。

7. 认证策划

7.1 审核方案策划

7.1.1 华亿认证应当针对每一认证客户建立认证周期内的审核方案，初次认证的审核方案应当包括两阶段初次审核、认证决定之后的监督审核和第三年在认证到期前进行的再认证审核。

注：一个认证周期通常为三年（有特定行业认证方案的除外），从初次认证（或再认证）决定算起，至认证的终止日期截止。

7.1.2 初次认证后的第一次监督审核应当在认证决定日期起12个月内进行,且两次监督审核间隔不超过15个月。在证书有效期内，应确保历次监督审核范围之和覆盖管理体系的全部范围。

7.1.3 华亿认证应当基于风险的方法进行审核方案策划，审核方案的确定和任何

后续调整应考虑客户的规模，其资管理体系有效性水平和以前审核的结果。

7.2 审核时间

7.2.1审核时间是指策划并完成一次完整且有效的管理体系审核所需的时间，包括从首次会议到末次会议之间实施审核活动的所有时间。

7.2.2 华亿认证根据参照CNAS-TRC-005：2010《审核时间指南》中，对认证机构策划审核方案时确定审核时间提供的指南，并根据PIIPMS审核工作量，在建立的HYC-ZY10《管理体系审核时间确认指南》文件中，提供了合理确定审核时间的框架，以便根据受审核方的特点确定合适的审核时间。该指南适用于单一体系审核或多体系一体化审核，也涉及了多场所组织审核。若有已发布或公认的计算方法（如CNAS、有关国际组织发布的方法），应当参照执行。华亿认证应当为每次审核计算个人身份信息保护管理体系认证实施规则认证审核时间，并留有记录。

管理体系初次认证审核的审核时间参照我机构ISMS的基础审核人日表查表确定，监督审核时间按照不低于初次审核的1/3计算,再认证审核时间按照不低于初次认证的2/3计算。

7.2.3 华亿认证应当建立并实施多场所认证抽样的规则，策划并保留多场所组织的抽样及计算审核时间的记录。

7.3 审核组

7.3.1 华亿认证应当根据组织申请认证的管理体系范围，组建具备能力的认证审核组，当审核组的专业技术能力不足时，可以配备该专业的技术专家。

7.3.2 技术专家主要负责提供审核组的技术支持，不作为审核员实施审核，不计入审核时间。

7.3.3 实习审核员应当在审核员的指导下完成审核，不计入审核时间，其在审核过程中的活动由负责指导的审核员承担责任。

7.4 审核计划

7.4.1 华亿认证应当为每次现场审核制定审核计划（一阶段审核除外）。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、时间安排和场所、审核组成员及审核任务安排。专业审核员和技术专家应当在审核计划中予以明确。

7.4.2 现场审核应当安排在受审核的组织的生产或服务处于正常运行时进行。

7.4.3 现场审核开始之前，应当将审核计划提交给受审核方并经其确认。如需要临时调整审核计划，应当经双方协商一致后实施。

7.5 与其他管理体系的结合审核

7.5.1 当评价指标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。

7.5.2 当个人身份信息保护管理体系认证实施规则认证审核在结合其他管理体系的认证审核时，总审核人日数应在按照CNAS-CC105计算结果的基础上，增加其他管理体系结合审核相应的人日数。

8. 审核实施

8.1 总要求

8.1.1 审核全过程应完整，不得增加、减少、遗漏认证审核规则程序。

8.1.2 审核组应当按照审核计划实施审核，形成相应记录，审核组可采用不同形式记录审核过程，如文字、图片、音像等。华亿认证应当保留相应记录。

8.1.3 审核组应当会同受审核方召开首、末次会议，受审核方的管理层及相关职能部门的人员应当参加会议。参会人员应当签到，审核组应当保留首、末次会议签到表（一阶段审核不做要求）。

8.1.4 发生下列情况时，审核组应当向华亿认证报告，经同意后终止审核。

（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。

8.2 初次认证审核

个人身份信息保护管理体系认证实施规则的初次认证审核应当分为两个阶段实施：一阶段审核和二阶段审核。

8.2.1 一阶段审核

实施第一阶段审核的基本条件：

- 受审核方的管理体系正式运行时间应不少于三个月；至少完成一次内部审核和管理评审，纠正措施已经关闭；

- 对从事国家实行许可制度或有关法律、法规规定必须取得相应的资格（许可）才能从事该类产品的生产、该类服务活动的受审核方，应具有相应的证明文件；

- 受审核方的管理体系文件已通过公司的文件初查，并确认文件更改已经完成，文件初查结论为“可进入现场审核”。

（1）一阶段审核应当收集信息，确定受审核方是否具备接受二阶段审核的条件。一阶段审核内容应当满足GB/T 27021.1《合格评定 管理体系审核认证机构要求 第1部分：要求》中相应规定。一阶段审核任务和目的具体包括：

a) 审核客户的文件化的管理体系信息；

b) 评价客户现场的具体情况，并与客户的人员进行讨论，以确定第二阶段的准备情况；

c) 审核客户理解和实施标准要求的情况，特别是对管理体系的关键绩效或重要的因素、过程、目标和运作的识别情况；

d) 收集关于客户的管理体系范围的必要信息，包括：

- 客户的场所

- 使用的过程和设备

- 所建立的控制的水平（特别是客户为多场所时）

- 适用的法律法规要求

e) 审核第二阶段所需资源的配置情况，并与客户商定第二阶段的细节；

f) 结合管理体系标准或其他规范性文件充分了解客户的管理体系和现场运作，以便为策划第二阶段提供关注点；

g) 评价客户是否策划和实施了内部审核与管理评审，以及管理体系的实施程度能否证明客户已为第二阶段做好准备。

上述一阶段审核的实施，需为第二阶段审核提供满足的基本条件：

- 第一阶段审核报告对受审核方的管理体系文件审核结论为“符合要求”或“基本符合要求”；

- 第一阶段审核报告的结论为“可安排第二阶段现场审核”。

（2）华亿认证应当制订文件以确定什么情况下可以不在受审核方现场实施一阶段审核。华亿认证应当记录未在受审核方现场开展一阶段审核的理由。

（3）华亿认证应将受审核方是否具备二阶段审核条件的书面结论告知客户，包括所识别的引起关注的、在第二阶段可能被判定为不符合的问题。

8.2.2 二阶段审核

（1）二阶段审核应当在受审核方的现场进行，评价受审核方管理体系的实施情况，包括对相应认证标准的符合性和体系的有效性。

（2）二阶段审核内容应当满足GB/T 27021.1《合格评定 管理体系审核认证机构要求 第1部分：要求》中相应规定。

8.3 监督审核

8.3.1 华亿认证应当对获证组织开展监督审核，以确认获证组织管理体系的持续符合性和有效性。监督审核应当在获证组织现场进行。

8.3.2 监督审核的内容应当满足GB/T 27021.1中相应要求，并重点关注变更以及绩效的持续改进。

8.3.3 由于市场、季节性等原因，在每次监督审核时难以覆盖所有产品和服务的，在认证证书有效期内的监督审核需覆盖认证范围内的所有产品和服务。

8.4 再认证审核

8.4.1 华亿认证应当根据获证组织的再认证申请实施再认证审核，以判断组织管理体系与相应认证标准的持续符合性和有效性。再认证审核应在认证证书到期前完成。

8.4.2 再认证审核的内容应当满足GB/T 27021.1《合格评定 管理体系审核认证机构要求 第1部分：要求》中相应要求。

9. 不符合纠正的验证

9.1 审核组应当根据审核发现形成严重或轻微不符合（见GB/T 27021.1中定义），要求受审核方在规定的时限内对不符合进行原因分析、采取相应的纠正和纠正措施（轻微不符合可以是纠正措施计划）。

9.2 对于严重不符合，华亿认证应当督促受审核方及时进行整改，并对其纠正和纠正措施的有效性进行验证。华亿认证应当规定严重不符合项的验证时限，并至少满足：

（1）初次认证：在二阶段审核结束之日起6个月内完成；

（2）监督审核：在审核结束之日起3个月内完成；

（3）再认证：在证书到期前完成。

9.3 对于组织未能在规定的时限完成对不符合所采取措施的情况，审核组不应当给予该受审核方推荐认证、保持认证或再认证。

10.审核报告

10.1 华亿认证应当就每次审核（一阶段除外）向受审核方提供完整详实的审核报告。审核组长应对审核报告的内容负责。

10.2 审核报告的内容应当反映受审核方个人身份信息保护管理体系认证实施规则的真实状况，描述对照相应认证标准的符合性和有效性的客观证据信息，及对认证结论的推荐意见。审核报告应当满足GB/T27021.1中相应要求，重点反映受审核方管理体系所取得的绩效，受审核方实际情况与其预期管理目标之间存在的差距和改进机会。

11.认证决定

11.1 华亿认证应当在对审核报告、不符合项的纠正和纠正措施及其结果以及其他信息进行综合评价的基础上，作出认证决定。认证决定人员应当为华亿认证管理控制下的人员，并不得为审核组成员。

11.2 经评定，华亿认证有充分的证据确认受审核方满足下列条件时，可做出授予认证的决定：

（1）具备应有的法定资格、资质；

（2）认证范围覆盖的活动、产品和服务符合相关法律法规要求，未发生重大事故和严重违法行为；

（3）对于严重不符合项，已评审、接受并验证了纠正和纠正措施的有效性；对于轻微不符合项，已评审、接受了受审核方的纠正和纠正措施或计划采取的纠正和纠正措施；

（4）受审核方的个人身份信息保护管理体系认证实施规则总体符合标准要求且运行有效的，对应审核组对受审核方的数据安全能力成熟度等级推荐，最终决定给予的成熟度等级。

11.3 经评定，华亿认证有充分的证据确认受审核方有以下情形的，应做出不授予

认证的决定:

（1）申请组织提供的审核材料明显涉嫌伪造，且关键岗位员工对管理体系不了解的;

（2）申请组织的实际情况与认证合同中约定的组织名称、地址、人员明显不一致的;

（3）申请组织申请认证的产品/服务超出经营许可范围或涉及生产许可、强制性认证等专项资质的;

（4）申请组织未开展内部审核及管理评审活动的。

11.4 授予组织的认证范围应当基于组织的法律地位文件及审核范围,不得大于其营业执照范围和行政许可范围以及审核范围。

11.5 再认证审核的认证决定宜在上一认证周期认证证书到期前完成,最迟应当在证书到期之日起6个月内完成。

12.认证证书

12.1 华亿认证应当向认证决定符合要求的组织出具认证证书,认证证书的生效日期不应早于认证决定的日期。

12.2 再认证证书的终止日期不得超过上一认证周期认证证书的终止日期再加三年。

12.3 认证证书载明的信息应清晰、明确、容易理解、设计上不会以任何方式产生误导。

12.4 认证证书中的获证组织及认证有关的信息应当真实、准确，不违反有关法规要求，至少包含以下内容:

（1）获证组织名称、注册地址，如经营地址与注册地址不同，还应注明经营地址。若认证的管理体系覆盖多场所,应表述认证所覆盖的所有场所的名称和地址信息(临时场所除外）;

（2）获证组织的管理体系所覆盖的产品、活动、服务的范围；

（3）认证依据的标准、技术要求；

（4）发证日期和有效期；

注：当证书失效一段时间时，华亿认证在满足下列条件时，可以在证书上保留原始的认证日期：

- 清晰标示了当前认证周期的开始时间和截止时间；
- 把上一认证周期截止时间连同再认证审核的时间一起标示。

（5）证书编号（或唯一的识别代码）；

（6）华亿认证名称、地址和认证标志；

（7）证书信息及证书状态的查询途径；

（8）认证标志的样式由基本图案、认证机构识别信息组成。本机构个人身份信息保护管理体系认证实施规则认证标志见图1所示：

华亿认证中心
HUAYI CERTIFICATION CENTER

图1 认证标志

13.认证证书的暂停和撤销

13.1 总则

13.1.1华亿认证应当制定暂停、撤销、恢复认证证书的管理规定，并遵照执行，不得随意暂停、撤销和恢复认证。

13.1.2 华亿认证应当在暂停、撤销或恢复认证决定生效后的2个工作日内，将相关信息报送至“CNCA认证认可业务信息统一上报平台系统”。

13.2 认证证书的暂停

13.2.1 获证组织有以下情形之一的,华亿认证应当在调查核实后的5日内暂停其认证证书:

(1) 管理体系持续或严重不满足认证要求的;

(2) 故意的或持续的不满足管理体系适用的法律法规要求的;

(3) 被有关执法监管部门责令停业整顿的;

(4) 发生重大事故/事件的;

(5) 拒绝配合执法监管部门的监督检查,或者提供虚假材料或信息的;

(6) 持有的与管理体系范围有关的行政许可证明、资质证书、强制性认证证书等过期失效的;

(7) 不能按照规定的时间间隔接受监督的;

(8) 未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的;

(9) 不承担、履行认证合同约定的责任和义务的;

(10) 主动请求暂停的;

(11) 其他应当暂停认证证书的。

13.2.2 华亿认证可以根据暂停的原因和性质规定暂停的期限,但暂停期限最长不得超过6个月。暂停到期后,华亿认证应当恢复或撤销认证证书。

13.2.3 华亿认证应当以适当方式公开暂停认证证书的信息,明确暂停的起始日期和暂停期限,并声明在暂停期间获证组织不得以任何方式使用认证证书、认证标志或引用认证信息。

13.2.4 在华亿认证规定的时限内,如果被暂停认证资格的组织采取了有效的纠正措施,造成暂停的问题已解决,华亿认证应当恢复被暂停的认证证书并保留相应证据。

13.3 认证证书的撤销

获证组织有以下情形之一的，华亿认证应当在获得相关信息并调查核实后5日内撤销其认证证书：

（1）被注销或撤销法律地位证明文件的；

（2）被执法监管部门认定存在严重违法失信行为的；

（3）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有效纠正的；

（4）其他应当撤销认证证书的。

13.4 证书等级的变更

特殊审核、监督或再认证，审核组现场审核确认获证组织的数据安全能力成熟度等级发生变更的，华亿认证应当在获得相关信息并调查核实后，经认证决定重新发放新等级认证证书。

14. 申诉、投诉处理

14.1 华亿认证应当建立必要的申诉、投诉处理程序。认证委托人对认证决定有异议时，可以向华亿认证提出申诉。任何组织和个人对认证过程和决定有异议的可以向华亿认证提出投诉。

14.2 华亿认证应当及时、公正、有效地处理申诉和投诉，必要时采取纠正措施。

15. 记录

15.1 华亿认证应当建立认证记录保持制度，记录认证活动全过程并妥善保存。

15.2 记录应当真实、准确，以证实认证活动得到有效实施。认证记录应当使用中文，存档留存时间为认证证书有效期届满或者被撤销之日起2年以上。

15.3 以电子文档方式保存记录的，应当采用不便于编辑的电子文档格式。

15.4 在认证证书有效期内，认证活动参与各方盖章或者签字的认证记录、资料等，

应当保持具有法律效力的原件。