受控

公有云中个人可识别服务信息保护管理体系认证实施规则

编　号：HNXH/CPIISMS-01-K/00

版　本：A0

编　制：技术部

修　订：技术部

审　核：

批　准：

2024年03月11日发布　　2024年03月11日实施

北京华诺信和认证有限公司

目录

公有云中个人可识别服务信息保护管理体系认证实施规则

一、适用范围

1.1 本规则用于规范依据 ISO/IEC 27018:2019 的标准要求对组织开展的公有云中个人可识别服务信息保护管理体系认证活动。

1.2 本规则依据认证认可相关法律法规、结合相关技术标准，对过程作出具体规定，明确机构、申请组织、获证组织责任，保证管理体系认证活动规范有效。

1.3 本规则适用于本机构在中国境内开展的公有云中个人可识别服务信息保护管理体系认证活动的基本要求，公司的员工、申请组织和获证组织等相关方应当遵守本规则。

二、认证机构要求

2.1 本机构是经国家登记主管机关依法登记注册、经中国国家认证认可监督管理委员会（CNCA）批准的第三方认证机构。

2.2 本机构依据国家标准GB/T 27021.1《合格评定管理体系审核认证机构要求》建立管理制度并符合其管理要求。

2.3 本机构已经建立内部制约、监督和责任机制，实现培训、审核和作出认证决定等工作环节相互分开，符合认证公正性要求。

2.4 本机构在行政许可和自身具备能力范围内提供认证服务。认证服务按照公认和适用的标准对申请组织的管理体系进行独立审核和认证，向所有申请方开放，不附加不正当的财务或其他条件。

三、认证人员要求

3.1 本机构参与公有云中个人可识别服务信息保护管理体系认证活动的认证人员应具备必要的个人素质和公有云个人可识别服务信息保护管理、技术管理等方面的教育、培训和（或）专业工作经历。

3.2 本机构参与公有云中个人可识别服务信息保护管理体系认证活动的认证人员应符合下述条件：

（1）公有云中个人可识别服务信息保护管理体系认证人员应通过公有云中个人可识别服务信息保护管理体系的培训。

（2）审核人员应取得中国认证认可协会的信息安全管理体系审核员注册的资格，并保持资格有效。

（3）认证人员应经本机构专业能力评定具备相应专业能力，方可开展相应职能工作。

3.3 认证人员应遵守从业相关的法律法规，对认证活动及作出的认证审核报告和认证结论的真实性承担相应的法律责任。

四、认证依据

ISO 27018:2019《信息技术 安全技术 基个人身份信息（PII)处理者在公有云中保护PII的实施规范》

五、认证模式

文件审核+现场审核+证后监督。

六、初次认证程序

6.1 受理认证申请

6.1.1 公开信息

本机构应向申请组织至少公开以下信息：

（1）可开展认证业务的范围，以及获得认可的情况。

（2）证书样式。

（3）对认证过程的申投诉规定。

（4）认证范围缩小、证书暂停及撤销制度。

（5）认证业务流程、

（6）联系地址及联系方式。

6.1.2 申请组织至少提交以下资料

（1）认证申请书，包括申请组织的生产、经营或服务活动范围和活动情况的说明。

（2）法律地位证明文件的复印件，例如：企业的法律地位证明文件为工商营业执照，组织申请认证的活动范围、生产或经营场所的数量和规模、地理位置，应附每个场所的法律地位证明文件的复印件（适用时）。

（3）资质证书扫描件及安全生产许可证（适用时）。

6.1.3 认证申请的评审

6.1.3.1 本机构对申请组织所提交的资料进行评审并保存评审记录，根据申请认证的活动范围、生产或经营场所、体系覆盖人数、完成审核所需时间和其他影响认证活动的因素，综合确定是否有能力受理认证申请。

对被执法监管部门责令停业整顿或在全国企业信用信息公示系统中被列入“严重违法企业名单”的申请组织，认证机构不应受理其认证申请。

6.1.3.2 对于符合 6.1.2 和 6.1.3 1 要求的认证申请，本机构可决定受理认证申请，并告知申请组织评审结果；对不符合上述要求的，通知申请组织补充和完善，或者不受理认证申请。

6.1.4 签订认证合同

在实施认证审核前，我机构应与申请组织订立具有法律效力的书面认证合同，合同应至少包含以下内容：