



公有云中保护 PII 的信息安全管理体系 认证实施规则

文件编号：GZ09

文件版号：H/0

北京中水卓越认证有限公司

H	0	马双	刘娜	付立华	2025-05-30
版号	修改号	编 写	审 核	批 准	批准日期

目 录

一、适用范围 3

二、认证机构要求 3

三、认证人员的要求 3

四、 认证依据 4

五、认证模式 4

六、初次认证程序 4

 1 受理认证申请 4

 2 审核方案策划 6

 3 实施审核 6

 4 审核报告 8

 5 不符合项的纠正和纠正措施及其结果的验证 9

 6 复核 9

 7 认证决定 9

七、监督审核程序 10

八、再认证程序 11

九、认证证书状态管理规定、要求 12

 1 通则 12

 2 暂停证书 12

 3 撤销证书 12

 4 认证证书信息公布 13

十、认证证书和认证标志要求 13

十一、受理转换认证证书 14

十二、受理组织的申诉 14

十三、认证记录的管理 14

十四、其他 15

一、适用范围

1. 本规则用于规范公有云中保护 PII 的信息安全管理体系认证活动。
2. 本规则依据认证认可相关法律法规，结合相关技术标准，对规范公有云中保护 PII 的信息安全管理体系认证过程做出了具体规定，明确公有云中保护 PII 的信息安全管理体系认证过程的相关责任，保证公有云中保护 PII 的信息安全管理体系认证活动的规范有效。
3. 本规则是本机构在公有云中保护 PII 的信息安全管理体系认证活动中的基本要求，公有云中保护 PII 的信息安全管理体系认证活动应当遵守本规则。

二、认证机构要求

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. 本机构依据国家标准 GB/T 27021《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。
3. 本机构建立内部制约、监督和责任制，实现公有云中保护 PII 的信息安全管理体系培训、认证和认证决定等工作环节相互分开，以符合公正性要求。
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方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、认证人员的要求

1. 本机构参与公有云中保护 PII 的信息安全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中保护 PII 的信息安全管理体系认证审核等方面的教育、培训和（或）工作经历。
2. 本机构参与公有云中保护 PII 的信息安全管理体系认证活动的认证人员应符合下述条件：
 - （1）公有云中保护 PII 的信息安全管理体系审核人员应取得中国认证认可协会的信息安全管理体系正式审核员资格，并保持资格有效；
 - （2）其他专职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）公有云中保护 PII 的信息安全管理体系专业同信息安全管理体系专业。
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

公有云中保护 PII 的信息安全管理体系认证依据：

ISO/IEC 27018:2019《信息技术 安全技术 公共云中作为个人身份信息处理者的个人身份信息(PII)保护的实践法则》

五、认证模式

文件审核+现场审核+证后监督

六、初次认证程序

1 受理认证申请

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。

1.2 申请组织应具备的基本条件

- (1) 通过了国家工商行政管理部门或有关机构的注册登记，建立和实施本体系并已运行 3 个月及以上；
- (2) 具有法人资格或其组成部分，能独立承担法律责任；
- (3) 一年内未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为“严重违法企业名单”；
- (4) 至少实施了一次完整的内审和管理评审。

1.3 递交申请

申请组织应向本机构提交书面申请，同时提交下述资料：

- (1) 认证申请书和承诺书；
- (2) 具有法律地位的证明文件（营业执照、组织机构代码证书扫描件）；
- (3) 行政许可证明文件（适用时）；

认证规则全文请联系公司综合部获取，联系人：刘岚，联系电话：010-58672798转8029