隐私信息管理体系认证规则

受控文件

修订日期：2026 年 10 月 22 日　　实施日期：2026 年 11 月 1 日

德世爱普认证(上海)有限公司 发布

目录

1 适用范围 3
2 认证依据及引用规范 3
3 对认证机构的基本要求 3
4 对认证人员的基本要求 4
5 认证程序 4
5.1 认证申请 4
5.2 申请评审 5
5.3 认证合同及相关责任 6
5.4 审核方案和审核策划 6
5.5 实施审核 8
5.6 初次认证审核 9
5.7 监督审核 10
5.8 再认证审核 10
5.9 特殊审核 11
5.10 不符合项及其验证 11
5.11 审核报告 11
5.12 认证决定 12
6 认证证书和认证标志 13
7 认证证书的暂停、撤销和注销 14
8 申诉（投诉）处理 15
9 信息公开与报告 16
10 认证记录 16
11 其他 17
12 附则 18
附件 A - 隐私信息管理体系认证业务范围分类与风险级别 19
附件 B - 隐私信息管理体系认证审核时间要求 20
附件 C - 隐私信息管理体系认证证书编号规则 23
附件 D - 隐私信息管理体系认证相关人员的资质要求 24

1 适用范围

本规则适用于德世爱普认证（上海）有限公司（以下简称 DQS）为中华人民共和国境内的场所提供的隐私信息管理体系（以下简称“PIMS”）认证服务。

1.1 为规范上述认证工作，根据《中华人民共和国认证认可条例》和《认证机构管理办法》等法律法规， 结合相关技术标准制定本规则。

1.2 本规则规定了 DQS 实施上述认证的程序与管理的基本要求，是 DQS 从事此认证活动的基本依据。

1.3 在中华人民共和国境内从事上述认证活动应遵守《中华人民共和国认证认可条例》《认证机构管理办法》及本规则。

1.4 认证机构遵守本规则的规定，并不意味着可免除其所承担的法律任。

2 认证依据及引用规范

2.1 认证依据：

ISO/IEC 27701 隐私信息管理体系标准。

2.2 引用规范：

- ✓ GB/T 27021.1 / ISO/IEC17021，
- ✓ ISO/IEC 27706-1;
- ✓ IAF MD1 。

3 对认证机构的基本要求

3.1 DQS 需获得国家认证认可监督管理委员会（以下简称“国家认监委 “ 或 CNCA）批准、取得上述认证领域的相关资质。

3.2 开展上述认证活动，应当围绕国家经济和社会发展目标，重点服务于经济社会高质量发展，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。

3.3 内部管理和认证活动符合 GB/T 27021.1 / ISO/IEC17021《合格评定 管理体系 审核认证机构要求 第 1 部分：要求》和有关 PIMS 认证能力要求，以确保 DQS 持续满足开展此认证的基本要求。

3.4 建立风险防范机制，对从事此认证活动可能引发的风险和责任采取合理有效措施。DQS 应对其开展的 PIMS 认证活动可能引发的风险进行了评估，对引发的责任做出了充分安排（如保险或储备金）。

3.5 建立认证人员管理制度，明确认证人员的能力准则、选择条件、聘用和评价程序，以及能力提升机制。确保从事此认证的人员持续具备相应职业素养和能力。 PIMS 相关的主要技术岗位的资质要求见附录 D。

3.6 在拟开展的上述认证的业务范围（认证业务范围分类见附录 A），具备不少于 1 名的专业领域审核员。DQS 结合认证业务范围识别相关专业的学历和专业信息安全工作经历。相应认证业务范围的专业领域审核员，应具备如下条件：

具有本科或以上学历：在信息安全或隐私信息管理相关领域有 2 年或以上的技术工作经历。

注:
部分认证规则在 DQS 网站上未显示全文。如需要获取全文，请联系我们：

德世爱普认证(上海)有限公司
Info.china@dqs.de；
021-62895083 - 22。