

朗实认证（北京）有限公司

关于“《信息安全管理体系认证规则》”客户告知函

尊敬的获证组织：

国家认证认可监督管理委员会(CNCA)于2026年1月14日正式发布了《信息安全管理体系认证规则》(CNCA-ISMS-01:2026)(以下简称《ISMS认证规则》),并于2026年3月1日起正式实施,届时我公司自行编制的信息安全管理体系认证规则自动失效。为确保贵组织平稳过渡至新版认证规则要求,保障认证活动的合规性、有效性。现将2026版《ISMS认证规则》的核心变化及与客户相关要求通告如下:

一、认证申请

(一) 认证申请条件(《ISMS认证规则》5.1.2条款)

提出认证申请时,认证委托人需要具备以下条件(包括但不限于):

1. 取得合法主体资格,并处于有效期内;
2. 取得相关法律法规规定的行政许可(适用时),并处于有效期内;
3. 已按认证标准建立ISMS,且运行满三个月;
4. 因获证组织自身原因被原发证机构暂停、注销或撤销ISMS认证证书已满一年(适用时);
5. 原ISMS认证证书发证机构被国家认监委撤销ISMS认证资质已满三个月(适用时);
6. 当前未被行政监管部门责令停产停业整顿;
7. 当前未列入“国家企业信用信息公示系统”和“信用中国”发布的严重违法失信名单;
8. 一年内未发生重大及以上级别的网络安全事件;

注:网络安全事件级别依据GB/T 20986判定。

9. 其他应具备的条件。

(二) 认证委托人应提供的信息和文件资料至少包括以下内容,并确保所提供的信息和文件资料真实有效:(《ISMS认证规则》5.1.3条款)

1. 认证申请,包括认证委托人的名称、地址、认证依据的标准、申请的认证范围、认证范围内人员数量及影响体系有效性的外包过程;
2. 法律地位的证明文件,当ISMS覆盖多个法律实体时,应提供每个法律实体的法律地位证明文件;
3. 申请认证范围所涉及的网络安全法律法规要求的行政许可文件、资质证书等(适用时);
4. 组织机构及职责;
5. 生产/服务的流程、班次及轮班情况;
6. ISMS运行满三个月的证据;
7. 一年内所发生的与网络安全相关的行政处罚以及整改情况(适用时);

朗实认证（北京）有限公司

8. 其他需要提供的文件。

二、认证合同及相关责任

(一) 认证合同及费用支付方式(《ISMS 认证规则》5.3.1 条款)

通过申请评审的, 认证机构应与每个认证委托人签订具有法律效力的认证合同, 明确认证服务的费用、付费方式和违约条款, 及认证委托人、认证机构和获证组织的责任。认证费用应由认证委托人向认证机构直接支付。

*认证委托人应向认证机构直接支付认证费用, 不得通过第三方支付。

(二) 认证委托人(拟申请认证组织)和获证组织的责任(《ISMS 认证规则》5.3.3、5.3.4 条款):

获证组织应遵守认证程序要求, 如实提供相关材料 and 信息, 通过 ISMS 认证后持续有效运行 ISMS, 配合认证行政监管部门的监督检查和认证机构对投诉的调查, 在广告、宣传等活动中正确使用认证证书、认证标志和有关信息, 及时向认证机构通报 ISMS 及“认证申请”中条件的变更情况, 承担选择的认证机构资质被撤销而带来的认证证书无法使用的风险。

三、审核安排要求

(一) 初次认证(《ISMS 认证规则》5.6.1 条款)

1. 初次认证的一阶段审核与二阶段审核, 时间间隔最短不得少于 5 日, 最长不得超过 6 个月;
2. 若因特殊情况需延长间隔时间, 需重新实施一阶段审核, 确保审核有效性。

(二) 监督审核(《ISMS 认证规则》5.4.1.4 条款)

1. 初次认证及再认证后的第一次监督审核, 需在认证证书签发之日起 12 个月内完成, 第二次监督审核应在认证证书签发之日起 24 个月内进行;
2. 两次监督审核的时间间隔不应超过 12 个月, 即本次监督审核的开始日期距上一次监督审核的结束日期不超过 12 个月;
3. 除再认证的年份外, 监督审核每个日历年需要进行 1 次;

(三) 再认证审核(《ISMS 认证规则》5.8.2、5.12.4)

再认证审核应在获证组织现场进行, 并应在认证证书到期前完成。不能在认证证书到期前完成现场审核的, 认证机构应按初次审核开展认证活动。

(四) 提前较短时间通知的审核(《ISMS 认证规则》5.9.2)

为调查投诉、重大及以上级别的网络安全事件、对变更作出回应或对被暂停的客户进行追踪, 可能需要在提前较短时间或不通知获证组织的情况下进行审核。

四、审核时间

(一) 审核时间计算标准(《ISMS 认证规则》5.4.2.1 条款)

1. 审核时间以“人日”为单位计算, 1 人日等同于 8 个有效工作小时;
2. 严禁通过延长单个工作日的工作小时数来减少审核人日数;

朗实认证（北京）有限公司

3. 若贵组织工作日的实际工作时间不足 8 小时，需配合延长现场审核天数，以满足规定的审核时间要求。

五、审核实施过程

（一）首末次会议参与要求（《ISMS 认证规则》5.5.3 条款）

1. 审核组应会同认证委托人召开首、末次会议；
2. 认证委托人的最高管理者、ISMS 相关职能部门负责人应参加首、末次会议，认证机构应保留首、末次会议签到记录、图片/音像证明材料。
3. 认证委托人的最高管理者不能参加首、末次会议的，应由获得书面授权的其他高级管理层成员参会，审核组应记录最高管理者缺席理由。

（二）最高管理者审核重点（《ISMS 认证规则》5.5.4 条款）

1. 审核组将通过面对面访谈等形式，重点审核贵组织最高管理者在 ISMS 中发挥领导作用的情况，并保留现场图片/音像、审核记录等证明材料；
2. 若出现以下情况，认证审核将直接不予通过：
 - 最高管理者不熟悉贵组织自身的信息安全方针、信息安全目标；
 - 最高管理者未亲自参与 ISMS 建设，或未推动 ISMS 有效实施。

（三）审核终止情况（《ISMS 认证规则》5.5.5 条款）。发生下列情况的，审核组应向认证机构报告后终止审核：

1. 认证委托人对审核活动不予配合，审核活动无法进行；
2. 认证委托人的最高管理者或经授权的高级管理层成员缺席首、末次会议；
3. 认证委托人实际情况与申请材料有重大不一致（《ISMS 认证规则》5.6.2.4 条款）；
4. 其他导致审核程序无法完成的情况。

六、认证证书和认证标志（《ISMS 认证规则》5.3.4、6.1.2、6.1.3、7.2、7.3、7.4）

（一）认证证书的有效期限最长为 3 年，对于未能在原认证证书到期前完成再认证决定的，获证组织的 ISMS 认证证书到期后自动失效，直至获得新签发的再认证证书，新签发的再认证证书的终止日期不超过上一认证周期终止日期再加 3 年。

（二）获证组织可以在认证证书有效时使用 ISMS 认证证书和认证标志，并接受认证机构的监督管理。认证证书处于暂停期间、被撤销或注销后，不得继续使用认证证书和认证标志。

（三）获证组织应当在广告等有关宣传中正确使用 ISMS 认证标志，不得在产品上仅标注 ISMS 认证标志，只有在注明获证组织通过 ISMS 认证及认证机构名称的情况下，方可在产品包装上标注 ISMS 认证标志。

（四）认证证书的暂停

获证组织有以下情形之一的，认证机构应在调查核实后 5 日内暂停其认证证书：

1. ISMS 持续或严重不满足认证要求的，包括 ISMS 文件与实际业务运作严重脱离；

朗实认证（北京）有限公司

2. 不满足 ISMS 适用的法律法规要求，且未采取有效纠正措施的；
3. 受到与信息安全相关的行政处罚，且尚未完成整改的；
4. 发生突发信息安全事件的；
5. 拒绝配合市场监管部门的认证执法检查监督，或者提供虚假材料或信息的；
6. 持有的与 ISMS 范围有关的行政许可文件、资质证书等过期失效的；
7. 不能按照规定的时间间隔接受监督审核的；
8. 未按相关规定正确引用和宣传获得的认证证书和有关信息，包括认证证书和认证标志的使用；
9. 不承担、履行认证合同约定的责任和义务的；
10. 被有关行政监管部门责令停产停业整顿的；
11. 发生与信息安全相关重大舆情的；
12. 主动请求暂停的；
13. 监督审核时发现的严重不符合的纠正措施未能在 3 个月内完成验证的；
14. 其他应暂停认证证书的。

（五）认证证书的撤销

获证组织有以下情形之一的，认证机构应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“国家企业信用信息公示系统”和“信用中国”列入严重违法失信名单的；
3. 认证证书的暂停期限已满，但导致暂停的问题未得到解决或有效纠正的；
4. 经行政监管部门确认因获证组织违规而造成重大及以上级别网络安全事件的；
5. ISMS 没有运行或者已不具备运行条件的；
6. 其他应撤销认证证书的。

七、认证记录的保存（《ISMS 认证规则》10.5）

获证组织应留存认证证书有效期内相应的认证记录，至少包括：

1. 认证合同；
2. 审核计划；
3. 首、末次会议签到表；
4. 不符合报告及原因分析和纠正措施；
5. 审核报告；
6. 暂停、撤销通知(适用时)。

朗实认证（北京）有限公司

八、我公司对获证组织的转换安排

由于《ISMS 认证规则》更新了认证证书的编号规则，所以自 2026 年 3 月 1 日起，所有获证组织的认证证书启用新版编号规则。对于已获证组织，我机构将结合最近一次监督/再认证实施转换，换发证书。

对于 2026 年 3 月 1 日以前签订的认证合同的组织，必须严格执行认证规则的要求，必要时，我公司将与贵组织签署补充协议或重新签署认证合同。

《ISMS 认证规则》是认证活动必须遵守的行政规范文件，请拟申请 ISMS 认证的客户及 ISMS 获证组织高度重视并认真学习。确保符合《ISMS 认证规则》的要求。ISMS 获证组织要提前与认证机构联系安排监督和再认证事宜，以免造成认证证书的暂停、撤销，影响证书使用。如有任何疑问，可随时与我机构总部(010-58090988)及各分支机构联系。

感谢贵组织长期以来对我公司的信任与支持!我们将全力协助贵组织完成认证规则实施过渡，共同保障认证活动的合规与高效。

附件：

1. 《信息安全管理体系统认证规则》(CNCA-ISMS-01:2026)
2. 《信息安全管理体系统认证规则》释义

下载网址：<https://www.cnca.gov.cn/>(下载页面：政务信息/公告/2026)

朗实认证(北京)有限公司

2026 年 02 月 28 日