关于实施 ISMS/ITSMS 认证规则的通知

尊敬的中润兴客户及各相关方：

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）和《信息技术服务管理体系认证规则》（CNCA-ITSMS-01:2026），并于 2026 年 3 月 1 日起正式实施。上述规则分别是 ISMS 和 ITSMS 认证活动的基本依据和底线要求，也是地方认证监管部门对获证组织及认证机构认证监管的重要依据。

为确保贵组织认证证书持续有效并符合上述《规则》的要求，现将相关的重点内容通告如下：

一、主要变化内容摘要

说明：未注明 “摘自 XX 规则” 的为 ISMS 和 ITSMS 两类认证的通用要求，申请任一体系均需满足。注明来源的为对应体系的专属要求，仅需根据所申请的认证体系，满足对应条款即可。

（一）认证申请阶段

1. 认证申请条件（《规则》5.1.2）

提出认证申请时，认证委托人应具备以下条件：

(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) 根据所申请的认证体系，满足对应要求：

申请 ISMS：已按 ISMS 认证标准建立体系，且运行满三个月（摘自 ISMS 规则）；

申请 ITSMS：已按 ITSMS 认证标准建立体系，且运行满三个月（摘自 ITSMS 规则）。

(4) 根据所申请的认证体系，满足对应要求（适用时）：

申请 ISMS：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（摘自 ISMS 规则）；

申请 ITSMS：因获证组织自身原因被原发证机构暂停、注销或撤销 ITSMS 认证证书已满一年（摘自 ITSMS 规则）。

(5) 根据所申请的认证体系，满足对应要求（适用时）：

申请 ISMS：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（摘自 ISMS 规则）；

申请 ITSMS：原 ITSMS 认证证书发证机构被国家认监委撤销 ITSMS 认证资质已满三个月（摘自 ITSMS 规则）。

(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。（仅 ISMS 适用，摘自 ISMS 规则）

(9) 其他应具备的条件。

2. 认证申请需提交的信息和文件资料（《规则》5.1.3）

认证申请需提交的信息和文件资料中特别需要注意以下资料的提交：

(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) 根据所申请的认证体系，满足对应要求
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；（摘自 ISMS 规则）
法律地位的证明文件，当 ITSMS 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。（摘自 ITSMS 规则）
(3) 根据所申请的认证体系，满足对应要求
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）；（摘自 ISMS 规则）
申请认证范围所涉及的信息技术法律法规要求的行政许可文件、资质证书等（适用时）；（摘自 ITSMS 规则）
(4) 组织机构及职责；
(5) 根据所申请的认证体系，满足对应要求
生产/服务的流程、班次及轮班情况；（ISMS 适用）
信息技术服务的流程、班次及轮班情况（ITSMS 适用）
(6) 所申请的管理体系运行满三个月的证据；
(7) （适用时）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。（仅 ISMS 适用，摘自 ISMS 规则）
(8) 其他需要提供的文件

（二）认证合同签署、费用支付及相关责任

明确了认证费用的支付要求以及认证委托人/申请组织额外的责任：

1. 合同签署和费用支付（《规则》5.3.1）

认证机构应与每个认证委托人（注：即申请认证的组织）签订具有法律效力的认证合同。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。认证委托人的上级单位（如认证委托人所属的集团公司、事业单位、社会团体或机关）或下级单位向认证机构支付费用是可接受的形式。

2. 认证委托人应承担的法律责任（《规则》5.3.3、5.3.4）

认证委托人应遵守认证程序要求，应如实提供相关材料和信息，配合认证行政监管部门的监督检查，及时向认证机构通报相应管理体系及认证申请条件的变更情况，并承担选择的认证机构资质被撤销而带来的认证活动终止、认证证书无法使用的风险。

（三）审核安排要求

1. 认证审核应在认证委托人的现场实施，包括初次认证审核以及认证周期内的每年度的监督审核、再认证审核和特殊审核。（《规则》5.5.1）

2. 初审审核：初次认证审核应分为两个阶段实施：第一阶段审核和第二阶段审核。两个阶段审核时间间隔最短不应少于 5 日，最长不应超过 6 个月。（《规则》5.6.1）

3. 监督审核：初次认证及再认证后的第一次监督审核应在认证证书签发之日起 12 个月内进行。此后，监督审核间隔不应超过 12 个月。第二次监督审核应在认证证书签发之日起 24 个月内进行。（《规则》5.4.1.4、5.4.1 释义、5.7.2）

4. 再认证审核：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，认证机构应按初次认证开展认证活动。（《规则》5.8.2）

5. 提前较短时间通知的审核：为调查投诉、突发事件，对变更做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。（《规则》5.9.2）

（四）审核时间 （《规则》5.4.2、附录 B）

1. 审核时间以“人日”计，1 人日为 8 小时，不应通过增加工作日的工作小时数以减少审核人日数。如果认证委托人工作日实际工作时间不足 8 小时，则应延长现场审核天数以满足审核时间要求。

2. 《信息安全管理体系认证实施规则》附录 B 信息安全管理体系认证审核时间要求有效人数与审核时间对照表中，相比认可规范（CNAS-CC170）新增 15 人以下单独档位的划分，认可规范中该人员区间分为两个档位。

3. 对于市场监管总局（国家认监委）或认可机构未明确审核时间要求的管理体系，ISMS/ITSMS 不能与其实施结合审核，也不能通过结合审核的方式减少审核时间。（《规则》5.4.2 释义 1）

（五）审核实施过程（《规则》5.5）

1. 首末次会议的参与要求（《规则》5.5.3）

认证委托人的最高管理者、管理体系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。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。

2. 最高管理者的审核重点（《规则》5.5.4）

审核组应通过面对面访谈等形式，对认证委托人的最高管理者在管理体系中发挥领导作用的情况进行重点审核，并保留现场图片/音像、审核记录等证明材料。最高管理者不熟悉组织自身的管理体系方针、目标，未亲自参与并推动管理体系实施的，认证审核应不予通过。

3. 审核终止情况（《规则》5.5.5、5.5.5 释义 4、5.6.2.4）

(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；

(4) 认证机构通过第一阶段审核发现相关申请信息和文件资料存在虚假情况的，应终止认证活动。

(5) 其他导致审核程序无法完成的情况。

（六）认证证书

1. 认证证书的有效期（《规则》6.2.1、6.2.3）

认证证书的有效期最长为 3 年。本规则实施后（2026 年 3 月 1 日起），新签发的再认证证书有效期也不得超过 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。

2. 认证证书编号规则（《规则》附录 C）

认证证书编号由认证机构代码、发证年份号、管理体系简写、顺序号、认证周期、认可机构代码和子证书号构成。

（七）获证后保持（《规则》5.3.4）

获证组织应遵守认证程序要求，如实提供相关材料和信息，通过认证后持续有效运行管理体系，配合认证行政监管部门的监督检查，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管理体系及“认证申请条件”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。

（八）认证记录保存（《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）。

（九）认证证书的暂停、撤销和注销（《规则》7.2、7.3、7.4）

1. 认证证书的暂停（《规则》7.2）

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，并保留相应证据：

(1) 管理体系持续或严重不满足认证要求的，包括文件与实际业务运作严重脱离；

(2) 不满足管理体系适用的法律法规要求，且未采取有效纠正措施的；

(3) 受到与网络安全相关的行政处罚，且尚未完成整改的（ISMS 适用，摘自 ISMS 规则）；受到与信息技术服务相关的行政处罚，且尚未完成整改的（ITSMS 适用，摘自 ITSMS 规则）

(4) 发生重大及以上级别网络安全事件，反映获证组织 ISMS 运行存在重大缺陷的（ISMS 适用，摘自 ISMS 规则）。

(5) 拒绝配合市场监管部门的认证执法监督检查，或者提供虚假材料或信息的；

(6) 持有的与相应管理体系认证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) 发生与相应管理体系相关重大舆情的；

(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。

2. 认证证书的撤销（《规则》7.3）

规则明确了撤销的认证证书失效，且不可恢复。明确了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 5 日内撤销其认证证书，并保留相应证据：

（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（ISMS 适用，摘自 ISMS 规则）；

（5） ISMS 没有运行或者已不具备运行条件的（ISMS 适用，摘自 ISMS 规则）；ITSMS 没有运行或者已不具备运行条件的（ITSMS 适用，摘自 ITSMS 规则）。

（6） 其他应撤销认证证书的。

3. 认证证书的注销（《规则》7.4）

获证组织主动申请不再保持认证证书时，认证机构应确认在不存在暂停或撤销情形后，注销其认证证书，并保留相应证据。

二、对贵组织的建议与要求

《规则》是认证活动必须遵守的法规性文件，对认证机构和认证客户均提出了更加明确和细化的要求。

请拟申请 ISMS 或 ITSMS 认证的客户以及获证客户高度重视，组织相关人员进行学习，充分了解认证工作的合规要求和风险，积极完善体系运行，提升人员能力，确保管理体系持续满足新版规则要求。并提前与认证机构联系安排认证事宜，以免造成认证证书的暂停、撤销，以及在地方认证监管部门中产生的监管处罚。

三、认真学习规则，共同遵守

认证规则是认证行业应遵守的法规性文件，对认证机构和认证委托人提出了明确的要求，请认证委托人和相关方高度重视、认真学习、深刻领会、共同遵守。

附件是《信息安全管理体系认证规则》（CNCA-ISMS-01:2026）和《信息技术服务管理体系认证规则》（CNCA-ITSMS-01:2026）全文及释义，敬请各相关方认真研读。我机构将持续提供支持，协助各方顺利过渡并符合新版规则的要求，助力组织提升管理水平。

附件 1:《信息安全管理体系认证规则》（CNCA-ISMS-01:2026）

附件2:《信息安全管理体系认证规则》释义

附件3:《信息技术服务管理体系认证规则》（CNCA-ITSMS-01:2026）

附件4:《信息技术服务管理体系认证规则》释义

北京中润兴认证有限公司

2026年02月13日