关于“信息安全管理体系认证新增国标依据”的客户告知函

各获证组织、公司各部门、全体审核员：

2025 年 6 月 30 日，国家市场监督管理总局、国家标准化管理委员会联合发布了 GB/T 22080-2025/ISO/IEC 27001:2022《网络安全技术 信息安全管理体系 要求》（以下简称“新版国标”），新版国标代替了 GB/T 22080-2016《信息技术 安全技术 信息安全管理体系 要求》，并于 2026 年 1 月 1 日实施。

新版国标等同采用 ISO/IEC 27001:2022《信息安全、网络安全和隐私保护 信息安全管理体系 要求》，并做了最小限度的编辑性改动。为确保各获证组织信息安全管理体系的持续合规与认证有效性，现将本次标准的核心变化、转换安排及注意事项通知如下：

一、主要变化

1、为与我国技术标准体系协调，认证依据的标准号及标准名称由“ISO/IEC 27001:2022《信息安全、网络安全和隐私保护 信息安全管理体系 要求》”改为“GB/T 22080-2025/ISO/IEC 27001:2022《网络安全技术 信息安全管理体系 要求》”；

2、纳入 ISO/IEC 27001:2022/Amd 1:2024《信息安全、网络安全和隐私保护 信息安全管理体系 要求》修正案 1:与气候行动相关的变化，并用双垂线在对应有变化的条款外侧标示。

3、其他描述见附件 1：GB/T 22080-2025 与 ISO/IEC 27001：2022 的差异性分析。

二、转换安排

1、2026 年 1 月 1 日起，本机构开始受理依据 GB/T 22080-2025/ISO/IEC 27001:2022 标准的信息安全管理体系初次和再认证申请。同时停止依据 ISO/IEC 27001：2022 标准的认证（初审和再认证）受理，所有审核活动均按新版国标要求实施；

2、已获证组织，将结合最近一次审核活动（包括监督审核、再认证、特殊审核）换发新版国标证书，标准转换不增加审核人日，审核组长应现场确认并收集企业已按新版国标更新的管理体系文件。

如有疑问，请随时联系我们，联系方式如下：
市场发展部：李老师，17857000517；赵老师，19817469297

附件 1：GB/T 22080-2025 与 ISO/IEC 27001：2022 的差异性分析

浙江盛标检测认证有限公司
2026 年 1 月 1 日

附件 1：GB/T 22080-2025 与 ISO/IEC 27001：2022 的差异性分析

条款号	条款内容	GB/T 22080-2025 与 ISO/IEC 27001:2022 的差异性分析
1	规定 ISMS 的建立、实施、维护和持续改进的要求	无差异
2	规范性引用文件	编辑性差异：引用标准编号不同，但技术内容通过等同采用（IDT）关系保持一致。
3	采用 ISO/IEC 27000 界定的术语和定义	无差异
4.1	明确影响信息安全管理系统预期结果能力的外部和内部问题	GB/T 22080-2025 明确要求“组织应确定气候变化是否是一个相关事项”
4.2	明确相关方的需求和期望	GB/T 22080-2025 在注释中说明相关方可能提出与气候变化相关的要求
4.3	规定确定范围的边界和适用性	无差异
4.4	要求组织建立、实施、维护和持续改进 ISMS	无差异
5.1	最高管理层应通过 a-h 活动证实其领导与承诺	无差异
5.2	最高管理者应通过 a-d 要求，并执行三条活动	无差异
5.3	最高管理者应确保信息安全相关角色的责任和权限得到分配和沟通	无差异
6.1	规划时应考虑风险和机遇，并定义和应用风险评估与处置过程	无差异
6.2	组织应建立信息安全目标，并在规划时确定如何实现	无差异
6.3	当确定需要对 ISMS 进行变更时候，应进行规划	无差异
7.1	组织应确定并提供所需资料	无差异
7.2	组织应确定、确保并保留人员能力的证据	无差异
7.3	人员应意识到信息安全方针、其贡献及不符合的后果	无差异
7.4	组织应确定内部和外部的沟通需求	无差异
7.5	组织应控制 ISMS 所需的文件化信息	无差异
8.1	组织应规划、实施和控制所需过程	无差异
8.2	组织应按计划执行信息安全风险评估	无差异
8.3	组织应实现信息安全风险处置计划	无差异
9.1	组织应监视、测量、分析和评价信息安全绩效和 ISMS 有效性	无差异
9.2	组织应按计划的时间间隔进行内部审核	无差异
9.3	最高管理层应按计划评审 ISMS	无差异
10.1	组织应持续改进 ISMS	无差异
10.2	发生不符合时，组织应采取措施并保留文件化信息。	无差异
附录 A	包含 93 项控制措施，分为组织、人员、物理、技术 4 类	无差异