信息安全管理体系认证实施规则

1. 目的和范围

本实施规则用于规范北京安信质联认证有限公司（以下简称“公司”）开展信息安全管理体系认证活动。制定本规则旨在结合认证认可相关法律法规和技术标准对审核信息安全管理体系实施过程作出具体规定，明确公司对认证过程的管理责任，保证认证活动的规范有效。

2. 认证依据

GB/T 27021.1-2017《合格评定 管理体系审核认证机构要求 第 1 部分:要求》

CNAS-CC170：2015《信息安全管理体系认证机构要求》

ISO/IEC27001-2022《信息安全管理体系要求》

3. 认证方法和审核方案

信息安全管理体系认证是依据相关认证标准，采用功能法对受评审方进行审核，确认满足认证标准要求后，通过出具认证证书证明其符合性的过程。

审核方案包括初次认证审核、第一年和第二年的监督审核及第三年认证到期前进行的再认证审核。第一个三年的认证周期从初次认证决定日算起。以后的周期从再认证决定日算起。

4. 认证基本程序

a） 认证申请

b） 申请评审

c） 文件审核

d） 初次现场审核（本文现场审核包含了采用电子手段进行远程审核以及在受审组织现场对其他场所实施的远程审核，如遇不可抗因素：目前全国范围内新冠疫情仍未得到完全控制，需规避人员流动传染的风险）

e） 认证决定与批准

f） 获证后的监督审核与再认证审核

5. 认证实施程序及要求

5.1 认证申请

在中华人民共和国境内注册的企业均可向公司提交信息安全管理体系认证申请。

由认证申请方填写《管理体系认证申请书》，并按其附件要求提供申请认证所需资料。资料包括，但不限于：

a） 组织简介；

b） 组织机构图；

c） 有效的企业营业执照；

d） 与企业活动有关的法律、法规（国际、国家、地方、行业）清单（可现场提供）；

e） 现行有效的信息安全管理体系文件及文件清单。

5.2 申请评审和方案策划

5.2.1 公司自收到认证申请方提交书面申请之日起十日内对申请资料进行评审，评审内容包括，但不限于：

a） 申请组织基本信息及其信息安全管理体系相关信息的充分性，了解组织特点，确定申请组织法律地位的合法性，必要时，通过公开网站验证提供信息的真实性、有效性；

b） 申请组织对于认证要求的信息是否已全部获知，并愿意遵守；对于认证要求的信息理解上的差异是否已得到解决。

c） 公司的专业能力是否满足审核实施的要求，包括认证审核人员和认证决定人员的能力是否满足要求；

d） 再认证审核申请要求与上一个认证周期的变更情况（再认证项目审核）；

对评审后确定无法受理的认证项目，公司将在 5 日内通知认证申请方。对不予受理的申请或认证申请方撤回的申请，应采取保密方式将申请文件和有关的资料归档保存。

5.2.2 认证合同的签订

公司授权人根据评审结论与认证申请方签署《管理体系认证合同》一式两份，公司和认证申请方各执一份。认证合同内容填写应完整、清晰、准确无误。

5.2.3 认证信息或认证要求变更申请的评审

获证组织提出组织名称、地址等的变更或认证要求的变更申请时，需填报《认证信息变更申请表》，并提交必要的补充信息。公司将对变更内容进行评审，且要特别关注其申请变更资料的充分性和合法性。经评审确认不能受理的，将及时反馈申请组织说明理由。

5.3 审核

5.3.1 审核准备