信息安全控制管理体系认证规则

文件编号：GZ25

文件版号：H/0

北京中水卓越认证有限公司

H	0	马 双	刘 娜	付立华	2025-05-30
G	0	魏树晗	刘 娜	陈洪征	2022-06-14
版号	修改号	编 写	审 核	批 准	批准日期

目 录

一、适用范围

1.本规则对信息安全控制管理体系认证过程作出具体规定，明确信息安全控制管理体系认证过程的相关责任，保证信息安全控制管理体系认证活动的规范有效。

2.本规则用于信息安全控制管理体系认证活动。

3.本规则是北京中水卓越认证有限公司（以下简称ZSBC）在ISC体系认证活动中的基本要求，信息安全控制管理体系认证活动应当遵守本规则。

4. 信息安全控制管理体系在下文中用ISC体系代替。

二、认证机构的要求

1.ZSBC 是经国家登记主管机关依法登记注册、经中国国家认证认可监督管理委员会（CNCA）批准的第三方认证机构。

2.ZSBC建立内部制约、监督和责任机制，实现认证决定等工作环节相互分开，以符合公正性要求。

3.ZSBC 提供的 ISC 体系认证可结合其他管理体系认证活动进行。

三、认证人员要求

1.本机构参与ISC体系的认证人员应具备必要的个人素质和信息技术认证审核等方面的教育和（或）工作经历。

2.本机构参与ISC体系认证活动的认证人员应符合下述条件：

（1）ISC体系审核人员应取得中国认证认可协会的信息安全管理体系正式审核员资格，并保持资格有效。

（2）其他专职认证人员应经本机构专业能力评定具备相应专业能力，例如了解特定的信息安全领域相关的信息安全风险，进行过相关领域的实践，方可开展相应职能工作。

（3）信息安全控制管理体系专业同信息安全管理体系专业。

3.认证人员应遵守从业相关的法律法规，对认证活动及作出的认证审核报告和认证结论的真实性承担相应的法律责任。

4.领导审核组应具备的能力要求：

（1）具备管理认证审核过程和审核组的知识和技能；

（2）备有效的口头和书面沟通能力。

应通过在有指导和监督下进行的审核来证实审核组长满足上述要求。

四、认证依据

认证依据：ISO/IEC 27002:2022《信息安全、网络安全和隐私保护-信息安全控制》

五、认证模式

认证模式：文件审核+现场审核+证后监督。

六、初次认证程序和要求

1 认证申请

1.1 申请组织具备基本条件

（1）取得国家工商行政管理部门或有关机构注册登记的法人资格（或其组成部分）；

（2）已取得相关法规规定的行政许可（适用时）；

（3）了解信息安全体系的法律、法规、政策和标准等；

（4）申请组织已建立信息安全体系且运行时间在 3 个月以上，审核前应至少进行一次完整的内审和管理评审；

（5）生产、加工的产品或提供的服务符合中华人民共和国相关法律、法规和有关规范的要求；

（6）在一年内，未发生违反国家相关法律法规，未因负面情况受到相关监管部门处罚或媒体曝光，或未因负面情况而被其他相关认证机构撤销管理体系认证证书。

1.2 申请组织提交的文件和资料

（1）认证申请书和承诺书；

（2）具有法律地位的证明文件（营业执照、组织机构代码证书扫描件）；

（3）行政许可证明文件（适用时）；

（4）ISC体系成文文件，如：管理策略、管理规定、实施细则、运行记录等。

（5）其他有关资料。

2 受理认证申请

2.1 申请评审

ZSBC根据申请认证的范围及场所、员工人数、完成认证活动所需时间和其他影响认证活动的因素，对认证申请组织提交的申请资料进行评审，并保存评审记录，综合确定是否受理认证申请。

2.2 评审结果处理