质诚嘉远（天津）认证有限公司

信息安全管理体系认证实施规则

文件编号：QIC-GZ-ISMS

版　　本：C/0

编　　制：技质部

审 核 人：李　丽

批 准 人：杨　平

目录

信息安全管理体系认证实施规则

1. 适用范围

为规范质诚嘉远（天津）认证有限公司（以下简称：QIC）在中国境内开展的信息安全管理体系（以下简称：ISMS）认证活动制定本规则。

2. 认证依据

2.1 ISO/IEC 27001：2022《信息安全管理体系 要求》；

2.2 当认证依据或法律法规变化时，认证机构将启动规则修订程序。

3 认证业务范围

ISMS 认证业务范围详见附录 A《ISMS 认证业务范围分类与分级》。

4. 对认证人员的基本要求

4.1 遵守认证认可相关法律法规及规范性文件的要求，具有从事认证工作的基本职业操守，对认证活动及其结果的真实性承担相应责任。

4.2 认证审核员应当取得国家认监委确定的认证人员注册机构颁发的信息安全管理体系审核员注册资格。

4.3 不得发生影响认证公正性的行为，应主动告知认证机构他们所了解的任何可能使其或认证机构陷入利益冲突的情况。因认证人员未履行告知义务而导致非公正性认证结果的，认证人员应当负有连带责任(如承担因此造成的经济损失)。

4.4 按要求接受人员注册/保持注册所要求的继续教育培训，以及机构要求的能力(包括知识和技能)提升活动，以持续具备从事 ISMS 认证工作相适宜的能力。

5. 认证程序

5.1 认证申请

5.1.1 QIC 向认证委托人至少公开以下信息：

（1）可开展认证业务的范围，获得认可的情况，以及分包境外QIC业务的情况；

（2）开展ISMS认证活动所依据的认证标准或其他规范性要求以及相关的认证方案、认证流程；

（3）授予、拒绝、保持、更新、暂停（恢复）或撤销认证以及扩大或缩小认证范围的程序规定；

（4）拟向组织获取的信息以及保密规定；

（5）认证收费标准；

（6）认证证书、认证标志及相关的使用规定；

（7）对认证过程和结果的申诉、投诉规定；

（8）认证标准换版的规定（必要时）；

（9）其他需要公开的信息。