万鼎认证（河南）有限公司
程序文件

编号：PD13-MS-B/1

认证风险管理与保密管理程序

编　　制：综合管理部

审　　核：张飞

批　　准：

受控状态：受控

发布日期：2025年12月15日　　实施日期：2025年12月31日

文件修改履历表				
版本	修改内容（条款）简述	提出	审核	批准/时间
1.0	新版发布	技术部	刘慧	王久新/2023.11.25
1.1	修正	技术部	刘慧	高俊/2024.4.20
B/0	版本号统一修订为B/0版，客户服务部变更为市场部；认证审核部变更为审核部；技术发展部变更为技术部；增加GB/T50430等	内审组/综合管理部	罗鹏	高俊/2025.2.14
B/1	根据CNCA-QMS-01:2025质量管理体系认证规则，局部内容修改。	技术部	张珍	高俊/2025.12.15

1 目的

为保证本机构认证风险的管理，以及申请我机构管理体系认证申请人的利益不受到损害，保护本机构作为第三方公正机构的形象和信誉，确保认证工作的公正性，同时确保认证信息的安全保密，特制定本程序。

2 范围

本程序适用于本机构在认证过程中所开展工作的认证风险管理（含公正性风险管理），及在进行此过程中接触到申请人的信息所做的保密工作。

2.1认证风险管理涉及到认证风险识别和风险控制措施，包括：

a)与本机构有业务关系的机构或相关机构；

b)与本机构认证业务有关的人员及其所从事的活动；

c)本机构在保持公正性方面所做的财务保障。

2.2保密范围涉及到：

a)在认证活动中获得的委托方和受审核方以书面（包括以各种媒体记录的信息）提供的申请文件内容和经济、技术数据等信息；

b)在现场审核活动中获得的受审核方的各种信息；

c)对受审核方管理体系能力和/或质量保证能力、服务能力的评价或结论等信息；

d)本机构与委托方和受审核方进行联系接触的动态信息；

e)本机构业务活动中经济往来的信息；

f)本机构的技术、管理等商业上的秘密。

3 引用标准或文件

《认证认可条例》

《质量管理体系认证规则》

CNAS-CC01《管理体系认证机构要求》

CNAS-EC-017《认证机构认可风险分级管理办法》

CNAS-RC02《认证机构认可资格处理规则》

万鼎《质量手册》

《风险评估管理办法》

4 职责

4.1总经理负责对认证活动的公正性做出声明，认证业务风险分析及风险处置报告，为风险处置提供资源。

4.2公司公正性委员会对公司的公正性管理和风险控制实施监督。

4.3管理者代表负责认证风险管理流程的建立，识别认证业务风险分析，组织制定风险处置措施，并编写报告；向公正性委员会报告公正性管理情况。

4.4技术部负责认证审核过程的风险控制结果的审议，并上报公司管理层并协助公司管理层实施风险识别和控制。

4.5各部门负责人对所辖范围内的保密工作负责；

4.6全体人员有责任和义务，按照本流程的要求，维护本机构的公正性及保密性。

5 认证风险管理

公司在所从事的认证及认证管理活动中，客观的存在着威胁公开性、有效性的风险，对于风险的控制和管理是公司管理层的职责，包括对脆弱点（威胁）的识别，风险的评价、风险控制措施的制定以及实施有效的管理。

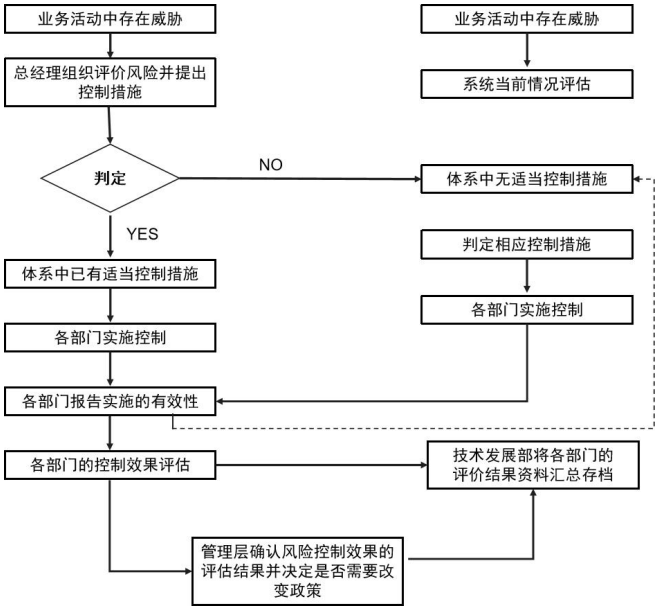
5.1风险评价过程

影响公正性/有效性方面的“威胁”的识别

脆弱点的识别→威胁的识别→风险评估和分级→风险控制措施的制定→实施控制措施使风险最低→现有的风险控制措施评审→风险可接受。

5.2认证活动中风险管理流程

认证活动中风险管理流程图



5.3认证风险管理程序

5.3.1威胁的识别

根据本公司现在和过去及将来认证活动的范围，主要从以下几个方面开展识别工作：

1) 自身关系的威胁；

a)公司所有者按其自身利益行为，作为公正性威胁，客观上存在关注的是自身财务利益；

b)公司作为认证机构在营销活动中会遇到处理与提供体系咨询的组织活动的关系(如咨询机构）等；

2)认证审核活动本身的威胁：

a)本公司所聘用的从事影响认证活动的人员可能给公正性带来威胁的行为；

b)认证审核活动本身客观上存在的审核风险：

(1)抽样的风险

(2)审核活动的风险

(3)审核活动控制的风险

(4)审核人员能力不足带来的风险等；

c)认证审核全过程管理中存在的风险

(1)申请评审结果的风险

(2)审核组的专业能力决定或配置过程中存在的风险

(3)认证决定过程中的风险等；

3)所从事的认证活动中所引发的产品责任和给机构带来的财务风险(管理体系认证审核活动中的责任风险）；

4)员工的职业健康安全问题所带来风险；

5)标志使用不规范的风险等。

5.3.2识别的方法

1) 询问、交谈

询问公司所有者、管理者、工作人员、审核人员、合作者等发现其存在的威胁；

2) 获取外部信息

全面了解认证行业的法律法规要求；

全面掌握业务领域的认可规范；

从同行业、文献资料、专家咨询获取有关威胁的信息。

3) 预先分析

在所从事的认证活动中做预分析和评估活动，识别潜在的威胁。

4) 威胁识别的调查

对于公司从事影响认证活动的人员要求其事先告之威胁的存在。

5) 现场观察和跟踪

对于认证全过程中所存在的风险其威胁的识别可通过现场的观察与跟踪调查。

6) 寻求法律顾问支持

公司可通过寻求法律支持的方式，科学的识别威胁的存在和将产生的风险程度。

5.3.3风险评价

公司总经理组织管理层人员识别各类威胁，通过公司的管理层讨论和审议、专家组审议、技术部讨论等方式，根据所识别风险的特点及现有的控制措施，组织开展相对应的风险评价，对于不可承受的风险还将视情况制定相应的专项控制措施方案。

5.3.3.1风险评价的依据

1）威胁所带来影响的程度和规模；

2）威胁出现的频次；

3）相关的法律、法规以及其他要求。

5.3.3.2风险评价的方法

公司制定了《风险评估管理办法》规定了风险评估的方法，常见的方法：

1)专家评议；

2)小组（技术部）讨论；

3)管理层讨论和审议；

4)律师建议函等。

公司可以采用一种或多种方法进行风险评价，并形成评价结果，由管理层委托公正性委员会秘书长上报公正性委员会实施对其公正性的监督管理。

5.3.3.3风险评价的分级

公司将风险分为1、2、3、4、5级别，其严重程度分别为轻微、可承受、中度、严重、不可承受,其中按照表1的风险评价矩阵图进行风险评价。

表1风险评价矩阵图

风险带来的严重程度	风险分级				
毁灭性的	3	4	4	5	5
非常严重	2	3	4	4	5
严重	2	2	3	4	4
一般	1	2	2	3	4
轻微	1	1	2	2	3
风险发生可能性	不会发生	可能性很小，小概率	有可能，不属于小概率	经常发生	极有可能

5.3.3.4不同类别界定

1)无需采取另外措施,严格执行现有的管理体系文件及管理制度;

2)无需采取特别控制措施,予以适当关注,通过体系文件及管理制度予以控制;

3)引起重视，一定时间内采取措施降低风险频率，必要时修改体系文件;

4)全面分析原因，引起领导重视，采取措施及时改进;

5)违反法律、法规及其他要求（如认证认可条例、认可规范等）；公司管理层特别关注的问题（如财务的支持、公正性）；政府、行业主管部门及相关方特别关注的问题；可能影响公正性的其他情况，一旦发生。引起领导层、公正性委员会、技术委员会的高度重视，制订系统、可行的解决方案，采取果断措施，立即消除此风险。

5.3.4风险控制

公司对风险的控制的主要途径：

1）对于轻微、可承受、中度、严重、不可承受，通过公司的日常系统管理，确保其对风险的控制;

a.制定管理程序或制度

b.培训与教育

c.制定应急预案

d.管理过程的监控

e.保持和改进现有措施

2）对于不可承受风险，识别后立即由总经理组织管理层人员制定相应的专项控制方案，通过实施各种措施等方式进行控制降到可接受风险，达到可接受风险程度，必要时建立专项管控方案来进行管控。

5.3.5可能采取的风险控制措施

5.3.5.1公司的最高管理层对机构的管理体系活动做出公正性承诺，并通过公正性承诺予以公开陈述,表明认证机构理解在实施管理体系的认证活动中公正的重要性以利于管理利益冲突和影响公正性的一切客观活动。

5.3.5.2公司的公正性委员会对公正性负有监督管理职责，公正性委员会成员各方代表利益均衡，在满足公正性要求的程序下的活动，确保监督职责的履行。

5.3.5.3公司管理层将向有关方以文件的形式陈述公司所从事的认证审核活动之间的关系。可能不造成利益冲突，当可能造成时，其风险控制措施将在其文件中做出规定。

5.3.5.4当咨询机构和本机构之间的关系对公正性拥有不可接受的威胁时，待管理体系咨询结束后至少2年，视将对公正性威胁降低到可接受水平的一种手段。

5.3.5.5本机构的营销活动中不与提供过体系咨询的组织活动相关（如咨询机构），公司将采取可行的措施避免对申请认证的组织宣称或暗示选择了某咨询机构认证简单，容易、快捷、优惠等。

5.3.5.6为了确保无利益冲突，提供管理体系咨询的人员，包括管理工作人员，在咨询结束后的2年内，不会被本机构聘用于对其参与过管理体系咨询的认证客户的审核或认证过程。

5.3.5.7本公司要求所有内部或外部的人员揭示他们知道的任何可能让他们本人或本机构陷入利益冲突的状况。公司将把该信息作为输入来识别被这些人或聘用他们而引发对公正性的威胁，未经说明无利益冲突不能聘用。

5.3.5.8公司对由于认证活动本身的风险导致所引发出的责任进行风险控制，通过设立专项风险基金的方式，对可能的赔偿予以财务上的支持，从而实现由于类似情况发生给公司财务运作带来的压力和经营风险。

5.3.5.9公司对于在认证审核过程中存在的审核风险，通过自身的管理体系进行全过程风险意识的培训和管理以及通过公正性委员会审定对审核全过程的风险实施控制。

5.3.6风险控制措施的评审

风险控制措施实施前应进行评审，主要考虑如下内容：

1) 风险控制措施是否将风险降至到可接受风险；

2) 风险控制措施是否带来新的威胁及残余威胁；

3) 风险控制措施是否适宜、可操作。

5.3.7风险识别及风险评价的更新

5.3.7.1更新的时机

1)法律、法规和其他要求发生变化；

2)业务领域的增加和公司管理模式的变化；

3)内审、外审和管理评审提出要求；

4)出现事故、事件或不合格；

5)相关方的抱怨或投诉等。

5.3.7.2年度评审

公司总经理每年在适当的时机组织管理层进行一次全系统的风险分析评价，并评价现有措施的有效性和评价是否需要进一步采取的措施。

5.4公正性管理

5.4.1公正性管理要求

5.4.1.1对本机构的要求

本机构除向申请人解释检查发现或阐明要求外，在任何情况下：

a）不主动或被动地向申请人提供为获得或保持认证的咨询服务；

b）不提供设计、实施或保持相应管理体系的服务，并确保不向任何申请人宣称或暗示使用了某个咨询机构/培训机构/个人的服务活动会给其带来任何商业上的、时间上的好处；

c）不提供、制造、安装、分销或维护我机构认证范围内的产品；

d）不设计、实施、提供或维护我机构认证范围内的服务；

e）不以申请人以少交、拒交或多交认证费用来影响认证决定的做出；

f）不因重要客户或合同额较大的认证项目而降低认证质量；

g）本机构不接受可能影响认证公正性的任何其他社会或个人的馈赠，并对本机构的各种经济利益关系、人员进行有效地控制，以使认证保持公正，和被视为保持公正，维护本机构作为公正的第三方的形象。

本机构对其认证活动的公正性负责，不允许商业、财务或其他压力损害公正性。如：不得将申请认证的组织（以下简称“认证委托人”）是否获得认证与参与认证审核的审核员及其他人员的薪酬挂钩。

5.4.1.2本机构对培训业务的控制

本机构在提供培训服务和作为教师参加与质量保证、管理体系、审核有关的课程时，仅限于提供在公开范围内可获得的一般信息和建议。

本机构公开其向外部提供的课程、培训内容、培训教材，并将其外部培训记录向CNAS公开。

5.4.1.3本机构对人员的控制

本机构确保高级主管和全体人员均免受任何有可能影响认证结果的商业、财务和其它方面的压力。

5.4.1.3.1公正性委员会成员

公正性管理委员会成员由认证机构的客户、获证客户的顾客、政府部门、非政府组织、消费者和其他公众、认证机构等与认证过程有关的各利益方代表和专家组成，认证机构的内部或外部人员视为一个利益方，其中任一利益方均不处于支配地位。来自同一单位的委员仅限于一

名代表，各方面的具体委员由相应的机构推荐产生。

5.4.1.3.2复核/认证决定人员

本机构管理体系审核的认证决定人员为授权的技术部人员实施。为确保其认证决定的公正性，要求参加对某一组织审核的成员、或其在过去两年内参与了向拟认证组织（或任何与该组织有联系的公司）提供任何咨询活动的成员，在对该组织作出认证决定时回避。

为确保本机构管理体系认证的复核及认证决定的公正性，要求参加对管理体系认证评价的复核及认证决定人员，不得参与对该项目的评价活动。反之亦如此。参与过对管理体系咨询的人员（包括管理岗位人员），在咨询结束后两年内，不得参与该项目的复核和认证决定。

5.4.1.3.3认证管理人员

本机构的审核活动由审核组组长负责，最后的认证决定由技术部成员做出。任何管理人员不能利用管理工作的便利条件对审核组组长、技术部的决定施加影响，而从影响公正性的决定。处理投诉或申诉的人员不能由与被投诉和申诉活动有关的人员进行。

5.4.1.3.4审核员

凡受聘为本机构的审核员必须做到：

a)本机构的专职审核员不得以任何名义从事认证咨询活动；

b)本机构的专职审核员不得应企业之邀为其提供内部管理体系审核；

c)曾在最近的两年内向拟认证的企业提供过咨询服务或近两年内曾在该企业任过职的审核员不得参与对该企业的认证活动；

d)在审核过程中和/或末次会议上，审核人员应解释审核发现和/或澄清审核标准的要求，但不应提出指示性建议或咨询。（可在审核时指出那些显而易见的改进机会而不是推荐具体的方法，以达增值服务的目的。）

同时本机构对审核员行为的进行以下方面监督与控制：

a)不得收受企业的礼品、礼金、有价证券和珠宝首饰等；

b)不得参加其审核企业安排的娱乐活动；

c)对食、宿、交通的特殊要求；

d)报销无关的票据；

在组成审核组时，审核员应填写《公正性声明、保密、诚信承诺书》以保证审核组现场审核的公正性。在审核结束后，应由受审核方确认《公正性声明、保密、诚信承诺书》的内容真实正确，以监督审核过程的公正性。当发现审核员有违上述各项公正性要求时或受审核方对审核员公正性行为向本机构进行投诉时，本机构将进行认证调查，严肃处理。

5.4.1.4本机构对不公平竞争行为的控制

本机构遵循公平竞争的原则开展认证业务，禁止采用诸如下述各种不正当的竞争手段：

a) 在公开文件中或签署认证合同前未向认证申请人明示本机构的认可业务范围而造成的误导；

b) 认证收费不参考发布的《认证收费标准》的规定；

c) 无正当理由全部或部分免收管理体系认证费用；

d) 以任何名义给予认证申请人或其代表回扣，给予中间人介绍费，并以此招来认证客户；

e) 与咨询机构达成给予介绍费等的任何协议或默契；

f) 与咨询机构/人员的咨询收费发生任何关系。

5.4.1.5财务运行及费用说明

我机构作为独立法人机构，有独立的财务账号和技术实力作为履行合同的必要保障，独立运作。我机构依据国家的相关规定制定收费办法，其收入用在以下方面：

a) 推动业务发展，如扩大业务范围；

b)人员晋升级及培训；

c)工资、劳务、办公（房租、办公用品及设备购置、差旅、技术文件及资料等）及管理所需费用。

d)所有费用均不作投资所用。

5.4.1.6本机构对相关机构的控制

对与本机构有共同的所有者、合同关系、名称中有共同的要素、非正式协定或其他关系的机构及与本机构有签约关系的分包检测机构等，均采用独立财务账号的方式进行控制，以避免对认证公正性和非营利的性质构成不利的影响。

5.4.2公正性管理的监视

5.4.2.1公正性委员会

本机构建立了公正性委员会，就影响公正性（包括公开性和公众认知）的事宜向委员会征询意见，同时邀请委员会对本机构公正性管理的情况进行审议。

公正性委员会成员由认证机构的人员和客户、获证客户的顾客、行业协会代表、政府监管部门或其他政府部门的代表，或非政府组织（包括消费者组织）的代表等与认证过程有关的各利益方代表和专家组成，认证机构的内部或外部人员视为一个利益方，其中任一利益方均不处于支配地位。来自同一单位的委员仅限于一名代表,各方面的具体委员由相应的机构推荐产生。具体见“公正性委员会章程”。

5.4.2.2公正性监视

本机构通过公正性委员会会议和日常沟通对公正性的工作进行监视。

公正性委员会每年度召开一次。相关负责人在年度会议上向委员会报告以下内容：

a)公正性风险评估及管理情况；

b)财务状况和收入来源,并证明其公正性始终没有受到商业、财务和其他方面压力的损害；

c)其他可能的威胁。

委员会委员结合报告内容，对本机构公正性管理情况进行审议。

认证业务涉及公正性事项时，本机构与公正性委员会委员进行日常沟通。沟通形式包括：邮件、电话，必要时组织临时会议。沟通的内容形成记录，并保存在综合管理部。

6 保密管理

6.1我机构的各类人员，包括公正性委员会委员、技术委员会委员、审核员、技术专家及各部门的人员，均应签订《认证人员公正性保证和保密承诺书》，明确责任及违反协议时应受的处罚，严守保密规定；公司有关部门、分公司、人员在实施认证过程中，应执行《认证风险管理与保密管理程序》，签署《公正性声明、保密、诚信承诺书》，对从事认证活动时获得或产生的所有信息予以保密。

6.1.1公司将拟对公众公开的信息提前告知客户。客户自己公开的信息除外，所有其他信息均应视为保密信息。本公司各级管理人员和审核人员应严格遵守以下保密纪律：

1)不向他人泄露客户的技术秘密；

2)不侵占或窃取客户的技术秘密资料；

3)不向无关人员谈论客户的审核工作情况或透露审核结果；

4)不对外泄露本公司的内部工作情况,严格控制与认证过程有关文件和资料的发放范围，按规定的范围发放有关文件，凡需保密的文件和资料及时归档保存。

6.2不得以任何方式（包括书面的和口头的）向他人泄露从与申请者接触中获得的有关管理体系、产品、服务、技术、管理、经济、经营等方面的信息，下列情况除外：

a)申请者曾公开的或向外透露过的资料；

b)接受申请或签订协议前，本机构已经拥有的有关申请者的资料；

c)申请者的上级合法机构要求了解的有关资料。

6.3对认证活动中所知悉的国家秘密、商业秘密负有保密义务。应通过在法律上具有强制实施力的协议，确保认证活动中所获得的信息在未经认证委托人书面同意的情况下，不向第三方透漏，认证行政监管有要求的除外。
6.4从其他来源（如投诉人、监管机构）获得的关于客户的信息，按保密信息处理。因工作需要需接触保密信息的人员，综合管理部组织相关人员对保密责任做出书面承诺。
6.5万鼎的人员，包括代表万鼎工作的任何委员会成员、合同方、外部机构人员或个人，除法律有要求外，应对从事万鼎的活动时获得或产生的所有信息予以保密。
6.6公司配备适用的设备设施（如档案柜、碎纸机、授权的ERP系统），确保保密信息得到安全处理。
6.7保密要求
6.7.1凡本公司专职及兼职工作人员，必须对所有非公开性文件、资料和信息保守秘密。未经本公司相关领导批准，不得私自复印、抄录、借阅、发放和保存。
6.7.2审核部委托审核组长向受审核方提交审核组成员签字的《公正性与保密声明》，并随审核资料留存在审核案卷中。任何人未经本公司书面许可不得在任何场合，以任何形式索要、复印、抄录和保存被审核方非公开性文件、资料和信息，包括被审核方审核中的信息。
6.7.3禁止在私人交往或通信中透露公司非公开性文件、资料和信息，禁止在公共场所谈论公司非公开性文件、资料和信息.
6.7.4公司员工一旦发现公司非公开性文件、资料和信息已经泄露或者可能泄露时，应当立即采取补救措施并及时通报公司总经理。
6.7.5每当项目任务结束后，各业务部门应将该项目的资料文件以及电子版内容交由综合管理部统一归档；全部审核资料与记录必须在规定的期限内归档。
6.7.6属于需保密的电子文件由综合管理部统一保存。
6.7.7采用电脑技术存储、处理、传递的保密资料，不得未经公司总经理批准，私自获取、复制、摘抄、收发、传递和外出携带。
6.7.8公司每位员工均需保密本业务领域的信息，不得泄露；与本人业务无关的人员不得打听和窃取。
6.8处罚规定
6.8.1员工出现下列行为之一，应予以警告，并扣罚50元以上500元以下绩效：
6.8.1.1泄露公司非公开性文件、资料和信息，尚未造成严重后果或经济损失的；
6.8.1.2已泄露公司非公开性文件、资料和信息但采取补救措施的。
6.8.2员工出现下列行为之一者，除按照保密合同规定内的条款进行处罚外，应予以辞退并酌情赔偿经济损失直至依法追究法律责任：
6.8.2.1故意或过失泄露公司非公开性文件、资料和信息，造成严重后果或重大经济损失的；
6.8.2.2为他人窃取、刺探、被他人收买或违反规定提供公司非公开性文件、资料和信息或利用职权强制他人违反规定的。
6.8.3发现失密、泄密现象、要及时报告。对失密、泄密者，给予1000-5000元的罚款。视情节轻重，公司给予行政处分，包括解除劳动合同；造成公司严重损失的，送有关机关进行处理。
6.8.4对于忠于职守，坚持原则，揭露失、泄密者，给予500-1000元的奖励。
7 质量索引记录
《认证人员公正性保证和保密承诺书》
《公正性声明、保密、诚信承诺书》