信息安全管理体系认证规则

文件编号：DNI-GZ-JS-26

文档版本：F/2

编制：技术部　　日期：2025.08.10

审核：杨　舒　　日期：2025.08.10

批准：申爱萍　　日期：2025.08.10

受控状态：受控文件

发布日期：2023年01月05日

修订日期：2025年08月10日

实施日期：2025年08月10日

发布单位：数网信认证服务（北京）有限公司

变更履历

日期	变更描述	版本/版次	审核	批准
2023.01.05	初始建立	A/0	杨舒	李静
2023.08.08	因CNAS申请修改多处内容	B/0	杨舒	李静
2024.09.19	组织架构及部门职责调整，文件版本与手册统一。	F/0	杨舒	申爱萍
2025.05.10	增加认证依据、审核策划、审核实施、认证证书及标志使用内容	F/1	杨舒	申爱萍
2025.08.10	增加发布单位。	F/2	杨舒	申爱萍

信息安全管理体系认证规则

1、适用范围

本认证规则适用于数网信认证服务（北京）有限公司（以下简称DNI）实施信息安全管理体系（以下简称ISMS）认证，满足第三方认证制度要求，作为提供认证服务的规则。必要时，在认证合同中补充相关的技术要求。

本认证规则在认证双方签订合同时予以确认和采用。

2、认证依据

ISMS认证依据为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》。

3、认证过程流程图、认证业务范围、认证审核员要求

1）认证过程流程图见附件一《管理体系认证业务流程图》。

2）依据《场监管总局关于在全国范围内推进认证机构资质审批“证照分离”改革的公告》（2022年第28号）的附件1以及公司现已获得资格的认证领域，ISMS领域为管理体系认证“04信息安全管理体系”。ISMS认证的认证业务领域按照CNAS-SC170进行划分，共计4个大类，30个中类进行，详见附件二。

3）认证审核员应取得中国认证认可协会（CCAA）的信息安全管理体系注册审核员资格。

4、认证申请及评审

4.1申请基本条件

认证客户具有明确的法律地位，客户具有企业营业执照、事业单位法人证书、社会团体登记证书、非企业法人登记证书、党政机关设立文件等，可独立申请认证。其他类型的客户，应由具备资格的单位代为申请，填写《管理体系认证申请书》。

国家、地方或行业有要求时，认证客户具有规定的行政认可文件，其申请认证范围应在法律地位文件和行政认可文件核准的范围内；申请的认证范围不能包括涉及国家安全和机密的内容和场所。

认证客户按相应的管理体系标准建立了文件化的管理体系（含适用性声明），初次认证现场审核前已至少持续稳定运行了3个月，至少已实施一次完整的内审和管理评审，并承诺在证书有效期内，持续有效运行管理体系。

认证客户承诺遵守国家的法律、法规及其他要求，承诺始终遵守认证的有关规定，承担与认证有关的法律责任，并有义务协助认证监管部门的监督检查，对有关事项的询问和调查如实提供相关材料和信息。

认证客户在一年内，未发生信息安全泄露事故（包括已经或可能严重损害国家安全、社会秩序、公共利益或获证客户及其相关方的合法权益）或被执法监管部门责令停业整顿或在全国企业信用信息公示系统中被列入“严重违法企业名单”或违反国家相关法规，虚报、瞒报获证所需信息的情况。

认证客户向 DNI 说明对认证机构资质要求或认证人员身份背景的要求，以及适用的与保守国家秘密或维护国家安全有关的法律法规要求，并说明是否存在因包含保密性或敏感性信息而不能提供给审核组核查的任何管理体系文件或记录的情况。

认证客户按照《管理体系认证申请书》要求提交申请资料时，受理人员应与申请人进行确认，提交资料是否包含申请组织保密性或敏感性信息。在不影响申请评审和文件审核的前提下认证客户可以对提交资料进行相应的处理，删除其中的保密性或敏感性信息。

认证客户承诺获得DNI认证后，按规定使用认证证书和认证标志和有关信息，不得擅自利用管理体系认证证书的文字、符号误导公众认为其产品或服务通过认证。按合同支付认证费用，并按规定接受监督。

认证客户承诺获得认证后按照DNI要求向DNI通报管理体系变更的信息和其他可能影响管理体系持续满足认证标准要求的能力的事宜的信息，一般包括：

a)客户及相关方有重大投诉；所提供信息安全服务被执法监管部门列入“黑名单”；

b)发生信息安全泄露事故；相关情况发生变更（包括：法律地位、生产经营状况、组织机构或所有权变更、资质证书变更；

c)法定代表人、最高管理者、管理者代表发生变更；

d)服务的工作场所变更；

e)管理体系覆盖的活动范围变更；

f)管理体系和重要过程的重大变更等；

g)出现影响管理体系运行的其他重要情况；

h)认证审核期间，认证客户不能够提供与拟认证范围相关的产品/服务/活动现场。

4.2申请评审

4.2.1公司通过申请评审活动以确保：

a）关于申请组织及其管理体系的信息足以建立审核方案；

b）解决了认证机构与认证客户之间任何已知的理解差异；

c）认证机构有能力并能够实施认证活动；

d）考虑了申请的认证范围、申请组织的运作场所、完成审核需要的时间和任何其他影响认证活动的因素(语言、安全条件、对公正性的威胁等)。

4.2.2 认证客户按照《管理体系认证申请书》要求提交申请资料，认证申请评审通过后，认证双方签订认证合同。如不受理认证申请，将及时通报认证客户。

5、审核实施

5.1审核准则

认证双方确认的审核依据如下：

1) 信息安全管理体系标准；

2) 审核准则还包括受审核方所适用的信息安全方针、目标、适用性声明、程序、标准、法律法规、操作规范、合同要求或行业规范。

5.2审核方案策划

公司对整个认证周期制定审核方案，以清晰地识别所需的审核活动，这些审核活动用以证实认证客户的管理体系符合认证所依据标准或其他规范性文件的要求。认证周期的审核方案应覆盖全部的管理体系要求。

初次认证审核方案应包括两阶段初次审核、认证决定之后的第一年与第二年的监督审核和第三年在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算起。以后的周期从再认证决定算起。审核方案的确定和任何后续调整应考虑客户的规模，其管理体系、产品和过程的范围与复杂程度，以及经过证实的管理体系有效性水平和以前审核的结果。

初次认证后的第一次监督审核应在认证决定日期起 12 个月内进行。此后，监督审核应至少每个日历年（应进行再认证的年份除外）进行一次，且两次监督审核的时间间隔不得超过 15 个月。

备注：为了考虑诸如季节或有限时段的管理体系认证（例如临时施工场所）等因素，可能有必要调整监督审核的频次。

如果考虑客户已获的认证或由另一认证机构实施的审核，则应获取并保留充足的证据，例如报告和对不符合采取的纠正措施的文件。所获取的文件应为满足本文件要求提供支持。公司根据获取的信息证明对审核方案的任何调整的合理性，并予以记录，并对以前不符合的纠正措施的实施进行跟踪。如果客户采用轮班作业，应在建立审核方案和编制审核计划时考虑在轮班工作中发生的活动。

5.2.1 审核时间

ISMS 审核人日参照 CNAS-CC170 进行，初次审核时间详见附件三《ISMS 体系有效人数与审核时间的关系表》。审核时间的确定要依据组织的管理体系有效人数、认证范围涉及的过程和活动的复杂程度、场所数量、审核类型等相关因素。审核时间主要包括文件评审、审核

准备、现场审核和最终报告等时间；不包括路途时间。通常情况下，监督审核的人日数按初审人日数的 1/3 计算，再认证审核的人日数按初审人日数的 2/3 计算。

5.2.2 多场所

若审核覆盖范围覆盖多个场所,这些场所的管理活动相似，且这些场所都处于申请组织的授权和控制下，可以根据多现场组织审核抽样的有关要求，在审核中对这些场所进行抽样。如果不同场所的管理活动存在明显差异，则不能采用抽样审核的方法，应当逐一到各现场进行审核。

对多个相似场所可进行抽样审核，抽样数量应不少于按以下方法计算的结果：

（1）初次认证审核：$Y=\sqrt{x}$

（2）监督审核：$Y=0.6\sqrt{x}$

（3）再认证审核：$Y=0.8\sqrt{x}$

注：其中 Y 为抽样的数量，结果向上取整；X 为相似场所的总体数量。

5.2.3 信息安全管理体系与其他管理体系结合审核

5.2.3.1 当 ISMS 认证审核和其他管理体系认证审核结合实施时，总审核人日数按照体系结合审核计算。与此同时，应符合其他管理体系认证方案的特定要求。

5.2.3.2 信息安全管理体系文件与其他管理体系文件的整合

客户可将信息安全管理体系文件与其他管理体系文件（如：质量管理体系）整合。如果体系文件是结合的，应能清晰地识别出客户的信息安全管理体系。

5.2.3.3 管理体系结合审核

信息安全管理体系与其他管理体系结合审核时，按以下管理要求执行：

1）对各体系分别界定审核范围。对审核时间的确定、审核方案策划进行有效管理。

2）必须以审核活动满足信息安全管理体系认证所有要求为前提，并且审核质量不应由于结合审核而受到负面影响。在审核报告中应清晰体现所有与信息安全管理体系有关的重要要素的描述。

5.2.4 审核准备

5.2.4.1 审核组

本机构根据 ISMS 认证覆盖的活动的专业技术领域选择具备相关能力的审核员组成审核组，必要时选择技术专家参加审核组，以提供技术支持。

5.2.4.2 审核计划

1）审核组长为每次审核制定书面的审核计划。审核计划包括以下内容:审核目的，审核准则，审核范围，现场审核的日期和场所现场审核持续时间，审核组成员等。

2）为使现场审核活动能够观察到相关过程的信息安全管理情况,现场审核将安排在认证范围覆盖的活动正常运行时进行。

3）在审核活动开始前,审核组长应将审核计划提交申请组织确认，遇特殊情况临时变更计划时，将通知申请组织有关变更情况，并协商一致。

5.3初次认证

5.3.1初次认证审核

初次认证审核分两个阶段实施：第一阶段和第二阶段。

第一阶段审核的目的是了解受审核方的基本信息、审核管理体系文件，识别任何引起关注的、在第二阶段审核中可能被判定为不符合的问题，为第二阶段审核提供关注点。

第二阶段审核的目的是评价受审核方管理体系实施的符合性和有效性。二阶段审核情况需进一步作出详细记录。

第一阶段必须到现场审核。

审核组对在第一阶段和第二阶段审核中收集的所有信息和证据进行汇总分析，评价审核发现并形成审核结论。

5.3.2第一阶段审核

审核组结合受审核方的管理体系运行目标和体系覆盖活动的专业特点，根据受审核方提供的管理体系文件、体系运作过程、运作场所和现场的具体情况、内部审核与管理评审策划和实施情况，确认受审核方对标准的理解和实施的程度、对目标的实现具有重要影响的关键点、相关的法律法规要求的遵守情况以及管理体系范围，审核第二阶段审核所需资源的配置情况，并与申请方商定第二阶段审核的细节，以确定第二阶段审核安排。确认：信息资产、风险分析及不可接受风险处置情况、信息安全服务的项目情况等。

评价组织是否策划和实施了内部审核与管理评审，以及管理体系实施的程度能否证明其已为第二阶段审核做好准备。

如果发生任何将影响管理体系的重要变更，DNI可能将重复整个或部分第一阶段审核。第一阶段审核的结果可能导致推迟或取消第二阶段审核。

5.3.3第二阶段审核

审核组现场评价受审核方管理体系的实施情况，包括符合性和有效性。第二阶段审核至少包括以下方面：

a） 与适用的管理体系标准和其他规范性文件的所有要求的符合情况；

b） 依据关键绩效目标和指标，对绩效进行的监视、测量、报告和评审；

c） 管理体系和绩效中与遵守法律有关的方面；

d） 受审核方过程的运作控制；

e） 内部审核和管理评审实施情况；

f） 管理职责的落实，包括针对方针的管理职责；

g） 为实现总目标而建立的职能层次目标的策划和实现情况；

h） 规范性要求、方针、绩效目标指标、适用的法律要求、职责、人员能力、运作、程序、绩效数据和内部审核发现及结论之间的联系。

信息安全管理体系还应包括：

a） 基于风险评估和风险处置过程，确定控制目标和控制；

b） 所制确定的控制、适用性声明、风险评估和风险处置过程的、信息安全方针、信息安全目标之间的一致性；

c） 控制的实施（控制措施），考虑了外部环境、内部环境与相关的风险，以及组织对信息安全过程及控制措施的监视、测量与分析，以确定控制是否得以实施，有效并达到其所规定的目标。

5.4审核实施

5.4.1公司策划审核过程，该过程包含从审核首次会议至末次会议的全部现场审核的过程。

5.4.2 召开首次会议

公司规定了首次会议需要陈述的事项，并编制了首次会议内容以提供给相关人员使用。首次会议通常由审核组长主持，会议的目的是简要解释将如何进行审核活动。详略程度可与客户对审核过程的熟悉程度相一致。

5.4.3审核中的沟通

5.4.3.1公司在对于审核组长的要求性文件中，要求审核组长应把握审核组定期评估审核的进程，并沟通信息。同时定期将审核进程及任何关注告知客户。

5.4.3.2 在现场出现可获得的审核证据显示审核目的无法实现，或显示存在紧急和重大的风险(例如安全风险)时，审核组长应向客户(如果可能还应向公司)报告这一情况，以确定适当的行动。当出现此种情况时，审核组应采取的行动，这可以包括重新确认或修改审核计划，改变审核目的或审核范围，或者终止审核。

5.4.3.3如果在现场审核活动的进行中发现需要改变审核范围，审核组长应与认证客户认真审查这个变更的需要，并上报公司，同时依据公司的相关控制要求进行处置。

5.4.4 获取和验证信息

5.4.4.1在审核中应通过适当的抽样来收集与审核目的、范围和准则相关的信息(包括与职能、活动和过程之间的接口有关的信息)，并对这些信息进行验证，使之成为审核证据。

5.4.4.2 信息收集方法应包括(但不限于)：

a.面谈；

b.对过程和活动进行观察；

c.审查文件和记录。

5.4.5 确定和记录审核发现

5.4.5.1审核发现应简述符合性，详细描述不符合以及为其提供支持的审核证据，并予以记录和报告，以便为认证决定，提供充分的信息。

5.4.5.2 识别和记录改进机会，除非某一管理体系认证方案的要求禁止这样做。但是属于不符合的审核发现不应作为改机会予以记录。

5.4.5.3关于不符合的审核发现，应对照审核准则的具体要求予以记录，包含对不符合的清晰陈述，并详细标识不符合所基于的客观证据。应与客户讨论不符合项，以确保证据准确。但是，审核员应避免提示不符合的原因或解决方法。

5.4.5.4 审核组长应协调、解决审核组与客户之间关于审核证据或审核发现的分歧意见，未解决的分歧点应予以记录。

5.4.6 准备审核结论

在末次会议前，审核组应进行内部沟通：

a.对照审核目的、审核发现和审核中收集的任何其他重要的信息；

b.考虑审核过程中的不确定性，就审核结论达成一致；

c.确定必要的跟踪活动；

d.确认审核方案的适宜性，或识别任何所需要的修改(例如范围、审核时间或日期、监督频次、能力)。

5.4.7 召开末次会议

5.4.7.1末次会议通常应由审核组长主持，会议目的是，提出审核结论，包括关于认证的推荐性意见。

5.4.7.2 末次会议还应包括下列要素，详略程度应与客户对审核过程的熟悉程度相关：

a）向客户说明所收集的审核证据基于对信息的抽样，因而会有一定的不确定性；

b）进行报告的方法和时间表，包括审核发现的分级(一般不符合、严重不符合)；

c）处理不符合(包括与客户认证状态有关的任何结果)的过程；

d）客户为审核中发现的不符合的纠正和纠正措施提出关闭的时间；

e）持续保持证书有效的要求，证书、标志的使用规定；

f）说明投诉处理过程和申诉过程。

5.4.7.3 客户应有机会提出问题。审核组与客户之间关于审核发现或结论的任何分歧意见应得到讨论并尽可能获得解决。任何未解决的分歧意见应予以记录并提交公司。

5.4.8 审核报告

5.4.8.1 审核组为每次审核提供书面报告，客户和机构各留一份。审核组可以识别改进机会，但不应提出具体解决办法的建议。审核报告的所有权归认证机构所有。

5.4.8.2 审核报告应提供对审核的准确、简明和清晰的记录，以便为认证决定提供充分的信息，并应包括或引用下列内容：

a）注明认证机构；

b）客户的名称和地址，活动范围和场所；

c）审核的类型(例如初次、监督、再认证或特殊审核)；

d）审核准则；

e）审核目的；

f）审核范围，特别是标识出所审核的组织或职能单元或过程，以及审核时间；

g）任何偏离审核计划的情况及其理由；

h）任何影响审核方案的重要事项；

i）注明审核组长、审核组成员及任何与审核组同行的人员；

j）审核活动(现场或非现场，永久或临时场所)的实施日期和地点；

k）与审核类型的要求一致的审核发现、对审核证据的引用以及审核结论；

1）如有时，在上次审核后发生的影响客户管理体系的重要变更；

m）已识别出的任何未解决的问题；

n）适用时，是否为结合、联合或一体化审核；

o）说明审核基于对可获得信息的抽样过程的免责声明；

p）审核组的推荐意见；

q）适用时，接受审核的客户对认证文件和标志的使用进行着有效的控制；

r）适用时，对以前不符合采取的纠正措施有效性的验证情况。

s）审核报告还应包含：

①关于管理体系符合性与有效性的声明以及对下列方面相关证据的总结：

——管理体系满足适用要求和实现预期结果的能力；

——内部审核和管理评审的过程。

②对认证范围适宜性的结论；

③确认是否达到审核目的。

5.4.9 不符合的原因分析

对于审核中发现的不符合，要求客户在规定的期限内分析原因，并说明为消除不符合已采取或拟采取的具体纠正和纠正措施。

5.4.10 纠正和纠正措施的有效性

按照要求审查客户提交的纠正和纠正措施及其实施情况。审核组应验证所采取的纠正和纠正措施的有效性，对不符合项的纠正及纠正措施，进行审查和验证，证据应予以记录。应将其结果告知客户。

5.5 认证决定

5.5.1 公司对所开展的认证做出授予或拒绝认证、扩大或缩小认证范围、暂停或恢复认证、撤销认证等认证活动进行控制。

5.5.2 作出认证决定前的行动

公司指定具有适宜能力的人作为认证决定人员，在做出认证决定前，对下列方面进行有效的审查，并应记录每项认证决定，包括从审核组或其他来源获得的任何补充信息或澄清：

a. 审核组促供的信息足以确认认证要求的满足情况和认证范围；

b. 对于所有严重不符合，已审查、接受和验证了纠正和纠正措施；

c. 对于所有轻微不符合，已审查和接受了客户对纠正和纠正措施的计划。

5.5.3 授予初次认证所需的信息

5.5.3.1 全部审核活动完成后，审核组应向公司提交完整的审核资料，包括以下信息：

a. 审核报告；

b. 对不符合报告的关闭意见，还包括对受审核方采取的纠正和纠正措施的意见；

c. 对已提供用于认证申请评审的信息的确认；

d. 对是否授予认证的推荐性意见及附带的其他条件或评论；

e. 对是否达到审核目的的确认。

5.5.3.2 如果不能在第二阶段结束后6个月内验证对严重不符合实施的纠正和纠正措施，则按照相关规定，在推荐认证前再实施一次第二阶段。

5.5.3.3 公司规定了在认证决定前对全套审核资料的审定要求，认证决定人员依据审定标准，对全套审核资料进行审定，并形成审定评价意见和结果。

5.5.3.4 实施审核的人员，不允许参与所审核项目的认证决定，应由公司授权的认证决定人员实施评审，总经理审批。

5.5.4 授予再认证所需的信息

公司按照所制定的相关文件，根据再认证审核的结果，以及认证周期内的体系评价结果

和认证使用方的投诉，做出是否更新的认证决定。

5.6 保持认证

公司在证实获证客户持续满足管理体系标准要求后保持对其的认证。按照认可规范的要求，在满足了下列前提条件的情况下，可以根据审核组长的肯定性结论保持对客户的认证，而无需再进行独立复核和决定：

1）对于任何严重不符合或其他可能导致暂停或撤销认证的情况，认证机构有制度要求审核组长向认证机构报告，并由具备适宜能力且未实施该审核的人员进行复核以确定能否保持认证；

2）由具备能力的认证机构人员对认证机构的监督活动进行监视，包括对审核员的报告活动进行监视，以确认认证活动在有效地运作。

5.7监督活动

5.7.1监督活动的方式

公司采用现场监督审核和日常监督（如关注国家有关部门发布的质量信息公报、关注获证客户相关方的信息、获证客户有关信息的日常跟踪、审查获证客户及其运作的说明、要求获证客户提供文件和记录等）相结合的方式。

5.7.2获证后监督审核的内容

a） 体系保持和任何变更情况（如资源、过程、组织结构、已识别的关键控制点等）

b） 顾客投诉的情况；

c） 涉及变更的范围；

d） 内部审核和管理评审；

e） 信息安全管理体系审核《适用性声明》及版本的变化情况；

f） 管理体系实施的有效性；

g） 为持续改进而策划的活动的进展；

h） 针对上次审核中确定的不符合所采取的措施和效果；

i） 证书和标志的使用和（或）任何其他对认证资格的引用；

j） 适当时，其他选定的范围。

获证客户应保存全部投诉记录，需要时提供认证机构。

DNI根据以上信息对获证客户管理体系进行再评价，确认其是否持续满足认证要求。对于监督审核合格的获证组织，做出保持信息安全管理体系认证资格的决定；否则，应暂停、撤销其相应的认证资格。监督审核时，如认证客户没有按要求关闭不符合，将可能导致认证证书的暂停。

5.7.3监督审核的频次

由于获证组织的（季节）业务特点及其内部审核安排等原因，可以合理选取和安排监督周期及时机，在认证证书有效期内的监督审核必须覆盖信息安全管理体系认证范围内的所有业务活动。

获证客户因未在规定的时间内实施监督审核而暂停认证证书的，监督审核恢复后，下次审核时间应按原计划时间计算。

若发生下述情况则需增加监督频次，或安排提前较短时间通知的审核：

1） 获证客户对管理体系进行了重大更改或发生重大问题；

2） 有足够信息表明获证客户发生了组织机构、服务变更等影响到认证基础的更改；

3） 获证客户出现信息安全泄露事故或用户提出对相关管理体系运行效果的投诉未得到处理时；

4） 其他需要考虑的情况。

5.8再认证

获证客户在证书有效期满前至少三个月，须提出再认证申请。再认证审核的目的是验证作为一个整体的组织管理体系全面的持续符合性和有效性，以及认证范围的持续相关性和适宜性。再认证审核的程序和要求参照5.4条实施。

在对获证客户的日常监督中，发现获证客户出现严重影响管理体系运作的重大变更时，或对获证客户的投诉分析和其他信息表明获证客户不再满足认证要求时，将安排特殊审核或与获证客户商定提前安排再认证审核。

再认证审核还需关注信息安全管理体系在认证周期内的绩效，包括调阅以前的监督审核报告。

对于多场所或结合审核的认证，再认证审核应确保现场审核具有足够的覆盖范围，以提供对信息安全管理体系认证的信任。

再认证时通常可不进行一阶段审核，但当获证客户的管理体系和获证客户的内外部运作环境有重大变化时，再认证审核活动可能需要有第一阶段审核。

再认证审核时，认证客户应在当前认证证书到期前接受审核，并对于审核组开具的不符合在规定的时间内按要求关闭。否则，因认证客户的原因导致不能在原认证证书到期后6个月内作出认证决定的，再认证审核失效。

5.9特殊审核

5.9.1扩大认证范围审核

针对已获证的客户，DNI对扩大认证范围的申请进行评审，确定能否予以扩大的决定所

需的审核活动，这项工作可与监督审核同时进行。

5.9.2提前较短时间通知的审核

为调查投诉、对变更做出回应或对被暂停的认证客户进行追踪，需要在提前较短时间通知获证客户后对其进行的审核。

1） 向获证客户说明并使其提前了解将在何种条件下进行此类审核；

2） 指派具有丰富经验的审核员组成审核组。

6、认证的批准、拒绝、保持、扩大、缩小、暂停、恢复和撤销的条件和程序

6.1批准认证范围的条件和程序

6.1.1批准认证注册的条件

1） 认证客户的申请材料真实、准确、有效；

2） 认证客户建立和实施的相关管理体系符合认证标准/规范性文件要求，审核组提出推荐认证的结论意见；

3） 认证客户申请认证范围在法律地位文件和资质规定的范围内；

4） 国家或地方或行业有要求时，认证客户申请认证范围内的组织单元、服务及其过程和活动已满足适用的法律法规的要求；

5） 审核证据表明管理评审和内部审核的安排已实施、有效且得到保持，并已进行了一次覆盖管理体系所有要求的完整内部审核；

6） 审核中发现的不合格在规定期限内已经采取纠正/纠正措施，经DNI验证有效。

7） 至少近一年来，认证客户申请认证范围内未发生信息安全泄露事故或国家检查不合格；

8） 认证客户已与DNI签署认证合同，承诺始终遵守认证的有关规定，并按照认证合同规定缴纳认证费用。

6.1.2批准认证资格的程序

1） DNI向认证客户提供认证有关信息的公开文件，使其知悉并理解；

2） 认证客户向DNI正式提交认证申请书和相关资料；

3） DNI根据客户申请信息进行申请评审，并已确认受理认证申请；

4） 满足6.1.1批准认证资格的条件，经DNI审定，认为认证客户在认证范围内已满足批准认证资格的条件，同意批准认证；

5） DNI向认证客户颁发认证证书，要求获证方按规定使用认证标志。

6.2拒绝认证注册的条件和程序

6.2.1拒绝认证资格的条件

1） 认证客户信息未通过DNI的申请评审，评审为不予受理认证申请；

2） DNI审核组现场审核结论为“不推荐认证注册”；

3） 初次认证第二阶段后，认证客户未在规定的时间内按要求关闭不符合，或未按规定接受DNI再次实施的二阶段审核；

4） 再认证审核后，认证客户未在规定的时间内按要求关闭不符合（包括DNI审定提出的不符合）；

5） 除以上情况外，DNI的审定结论为不予认证注册。

6.2.2拒绝认证注册的程序

1） 符合6.2.1条件之一，经DNI评审为不予受理认证或认证客户的管理体系不满足批准认证资格条件；

2） DNI向认证客户发出《不予认证注册通知》。

6.3保持认证资格的条件和程序

6.3.1保持认证资格的条件

1） 获证客户的法律地位、行政许可文件持续符合国家的最新要求，并且认证范围在法律地位文件和行政许可文件规定的范围内；

2） 获证客户持续遵守认证有关的规定，包括变更的规定；

3） 获证客户在认证范围内的组织单元、服务及其过程和活动持续满足适用的最新法律法规的要求，如发生不满足时及时采取有效的措施；

4） 获证客户于获证期内，认证范围内涉及的服务/活动未发生重大事故和国家检查不合格；

5） 获证客户在获证期间未发生误用认证证书和认证标志，如有发生能及时有效地采取纠正和纠正措施，并将误用产生的影响降至最少程度；

6） 获证客户对顾客或相关方的重大投诉和关切能及时有效地处理；

7） 获证客户能按照DNI要求及时通报管理体系和重要过程变更等信息；

8） 按时接受监督审核,经现场审核获证客户的管理体系持续符合认证标准/规范性文件要求，审核组结论为“保持认证”；

9） 获证客户履行与DNI签署认证合同中规定的责任和义务，并按照认证合同规定缴纳认证费用。

6.3.2保持认证资格的程序

1） 满足6.3.1保持认证资格的条件，监督审核后，经DNI派出的审核组长确认和DNI审查后认为获证客户在认证范围内能持续满足保持认证资格的条件，同意保持认证资格，由

DNI 签发确认证书并向获证客户发放；

2） 在认证证书有效期内如有认证要求变更，获证客户接受变更的认证要求，并经DNI验证在认证范围内管理体系满足变更的要求，可保持认证资格。

6.4扩大认证范围的条件和程序

6.4.1扩大认证范围的分类

1） 获证客户名称增加、固定分场所增加、服务点增加；

2） 服务类别增加；

3） 服务形成主要过程增加，如软件设计开发服务、软件测试服务。

6.4.2扩大认证范围的条件

1） 获证客户保持认证资格有效。

2） 获证客户申请扩大的认证范围在法律地位文件范围内。国家、地方或行业有要求时，获证客户拟扩大的认证范围具有有效的行政许可文件；

3） 国家或地方或行业有要求时，获证客户在申请扩大认证范围内的组织单元、产品、服务及其过程和活动，已满足适用的法律法规的要求；

4） 获证客户的管理体系覆盖申请扩大的认证范围，并符合认证标准/规范性文件要求

5） 获证客户按照认证规定缴纳补充认证费用。

6.4.3扩大认证范围的程序

1） DNI向获证客户提供与扩大认证范围有关信息的公开文件，获证客户知悉并理解；

2） 获证客户向DNI正式提交扩大认证范围的申请和相关资料；

3） 需要时，获证客户与DNI补充签署或修订认证合同，按照规定补充缴纳认证费用；

4） 满足6.4.1扩大认证范围的条件，经DNI审核、审定，认为获证客户在申请扩大认证范围内已满足批准认证资格的条件，同意批准扩大认证范围，认证证书的注册号和有效期保持不变；

5） DNI向获证客户送交新认证证书，同时收回原证书。

6.5缩小认证范围的条件和程序

6.5.1缩小认证范围的分类

1） 获证客户固定分场所缩小；

2） 服务类别减少；

3） 服务形成主要过程减少，如软件设计开发服务、软件测试服务；

4） 多个组织认证减少组织数量。

6.5.2 缩小认证范围的条件

1） 获证客户认证范围内部分产品/服务、区域等不再符合认证标准/规范性文件和其他要求；

2） 获证客户不愿再继续保持认证范围内的部分服务、区域等认证资格；

3） 获证客户缩小认证范围应不包括为缩小认证风险的情况。

4） 如果获证客户在认证范围的某些部分持续地或严重地不满足认证要求，DNI将缩小其管理体系认证范围。以排除部门组要求的部分。认证范围的缩小应与认证标准的要求保持一致。

6.5.3 缩小认证范围的程序

1） 获证客户向DNI正式提交缩小认证范围的申请，或DNI提出缩小获证客户认证范围的建议，并提供理由和证据。DNI的审定意见和日常监督结果也可作为认证范围缩小的信息来源和理由，经认证双方沟通后达成一致意见；

2） 需要时，获证客户应与DNI修订认证合同；

3） 经DNI审定，认为获证客户申请缩小认证范围不会对仍保持的认证范围产生影响，同意批准缩小认证范围，换发认证证书或附件，认证证书的注册号和有效期保持不变。

6.6变更认证信息的程序

1） 获证客户应根据要求向DNI正式提出申请和相关文件资料；

2） 需要时，获证客户应接受DNI的审核；

3） 经DNI审定，认为获证客户满足认证信息变更的条件，同意批准认证信息变更；

4） DNI换发认证证书或附件，认证证书的有效期保持不变。

6.7暂停认证资格的条件和程序

6.7.1暂停认证资格的条件

符合下列条件之一的获证客户，DNI将暂停其认证证书：

——获证客户管理及服务体系持续或严重不满足认证要求，含对管理体系运行有效性要求；

——获证客户的管理体系发生重大变更，不能持续符合认证标准/规范性文件要求；

——获证客户监督审核期间发生严重影响体系运行的情况；

——获证客户在认证范围内的组织单元、服务及其过程和活动不能满足适用的DNI提出对获证客户暂停全部或部分认证范围内认证资格的建议，并提供最新法律法规和标准要求，并未采取措施或措施无效；

——获证客户未按照认证要求的变更做出相应调整，或调整不满足变更要求；

——获证客户不承担、履行认证合同约定的责任和义务；

——获证客户未能在规定的期限内接受监督或再认证审核；

——获证客户未履行与DNI签署认证合同中规定的责任和义务，并对保持认证资格产生重大影响；

——获证客户未按照认证合同规定缴纳认证费用；

——获证客户在获证期间发生误用认证证书和认证标志，并未能及时有效地采取纠正和纠正措施，以将产生的影响降至最少程度；

——获证客户在证书有效期间受到相关执法监管部门处罚；

——获证客户未按要求对信息进行通报；

——获证客户被地方认证监管部门发现体系运行存在问题；

——获证客户于获证期间在认证范围内发生国家抽检不合格，并未查明原因和采取补救措施；

——获证客户持有的行政许可证明、资质证书、强制性认证证书等过期失效，重新提交的申请已被受理但尚未换证；

——获证客户的法律地位、资质不再符合国家的最新要求；

——获证客户的认证范围已不在现行有效的法律地位文件和资质规定的范围内，但仍有可能在短期内符合规定要求；

——获证客户不接受或不配合认证认可监督管理部门的监督管理；

——获证客户主动请求暂停；

——获证客户发生了与信息安全泄露事故或与其有关的重大事故，反映出获证客户的体系建立及运行存在重大缺陷；

——获证客户于获证期间在认证范围内发生重大事故被媒体曝光、或未查明原因和采取补救措施；

——获证客户服务出现严重波动，未采取措施；

——其他原因需要暂停证书。

6.7.2暂停认证资格的程序

1） 提出对获证客户暂停全部或部分认证范围内认证资格的建议，并提供理由和证据，或由获证客户向DNI提出暂停认证资格的申请；

2） 必要时，DNI与获证客户沟通，核实证据；

3） 经DNI审定，认为获证客户在认证范围内全部或部分不再持续满足认证要求，但仍然有可能在短期内采取纠正措施的，同意批准暂停全部或部分认证范围的认证资格，并确定暂停期限，向获证客户颁发《暂停认证资格通知书》并公告；

4） 获证客户停止使用认证证书和认证标志，

在暂停期间，客户的管理体系认证暂时无效。

6.7.3暂停期限

认证资格暂停期最长不超过6个月。

6.8恢复认证资格的条件和程序

6.8.1恢复认证资格的条件

获证客户已针对暂停认证资格的原因采取了有效的纠正措施，产生原因已经消除，认证资格的恢复符合相关的认证要求，同时已证实在暂停期内没有使用、引用认证资格（如广告宣传）和使用认证标志。

6.8.2 恢复认证资格的程序

1） 在确定的认证资格暂停限期结束前，根据暂停原因，获证客户在规定期限内向DNI提出恢复认证资格的申请；

2） 需要时，获证客户应提交相关纠正措施和有效性验证材料；

3） 经DNI审定，确认获证客户在暂停认证资格的认证范围内已恢复符合相关认证要求，做出同意恢复认证资格的结论，告知客户并公告。

6.9 撤销认证资格的条件和程序

6.9.1 撤销认证资格的条件

符合下列条件之一的获证客户，DNI将撤销其认证证书：

——获证客户审核未通过；

——获证客户被注销或撤销法律地位证明文件。获证客户的法律地位、资质不再符合国家的最新要求；

——获证客户拒绝配合认证监管部门实施的监督检查，或者对有关事项的询问调查提供了虚假材料或信息；

——获证客户出现重大的信息安全泄露事故等，经执法监管部门确认是获证客户违规造成；

——获证客户于获证期间在认证范围内发生国家抽检不合格，并造成严重影响；

——获证客户在证书有效期间有其他严重违反法律法规行为，受到相关执法监管部门处罚；

——获证客户暂停认证证书的期限已满，但导致暂停的问题未得到解决或纠正（包括持有的行政许可证明、资质证书、强制性认证证书等已经过期失效但申请未获批准）；

——获证客户没有运行管理体系或者已不具备运行条件；

——获证客户在认证范围内的管理体系发生重大变更，未向DNI通报，并在短期内无法满足认证要求；

——获证客户体制变更后原管理体系已不再适宜；

——获证客户不再进行体系覆盖内的信息安全服务；

——获证客户在认证范围内的组织单元、服务及其过程和活动严重不能满足适用的最新法律法规和标准的要求，并在短期内无法采取措施或采取措施无效的；获证客户停业或关闭的；

——获证客户不按相关规定正确引用和宣传获得的认证信息，造成严重影响或后果，或者认证机构已要求其纠正但超过2个月仍未纠正；

——获证客户在获证期间发生大量误用认证证书和认证标志，并未能及时有效地采取纠正和纠正措施，误导消费者，影响面大；

——获证客户转让认证证书和认证标志；

——获证客户发生了与信息安全泄露事故或有关的重大事故，反映出获证客户的体系建立及运行存在重大缺陷；

——获证客户因换发新证而撤销旧证书；

——获证客户不承担、履行认证合同约定的责任和义务；

——获证客户单方面宣布不履行与DNI签署认证合同中规定的责任和义务的；

——获证客户长期拖缴认证费用，并催缴无效的；

——经核实获证客户提供虚假信息，且影响了审核、认证决定的有效性的；

——获证客户更换认证机构的（未书面告知DNI的）；

——获证客户对顾客或相关方的重大投诉不做处理的；

——获证客户主动放弃认证；

——其他原因需要撤销证书。

6.9.2撤销认证资格的程序

经DNI核实与审定，确认获证客户在认证范围内的管理体系不再满足认证要求，作出撤销认证资格的结论，发放《撤销认证资格通知书》并公告，同时收回认证证书，认证客户不得再使用认证证书和认证标识。。

7、认证证书和认证标志要求

7.1 认证证书应至少包含以下信息：

1）获证组织名称、地址和统一社会信用代码，该信息应与其法律地位证明文件的信息一致；

2）信息安全管理体系覆盖的生产经营或服务的地址和业务范围。若覆盖多场所，表述覆盖的相关场所的名称和地址信息；

3）信息安全管理体系符合标准的表述；

4）证书编号；

5）认证机构名称；

6）有效期的起止年月日，证书应注明：获证组织必须定期接受监督审核并经审核合格此证书方继续有效的提示信息；

7）证书查询方式。认证机构除公布认证证书在本机构网站上的查询方式外，还应当在证书上注明：“本证书信息可在国家认证认可监督管理委员会官方网站（www.cnca.gov.cn）上查询”，以便于社会监督。

7.2 认证证书有效期最长为3年。认证样本见附件四。

7.3 公司对获证客户使用的标志的进行管理，并满足认可准则和规范的要求。标志或所附文字不应使人对获证组织和公司产生歧义。认证的标志不应用于产品或消费者所见的产品包装之上，或以任何其他可解释为表示产品、过程或服务符合性的方式使用。且不应允许其标志被获证客户用于实验室检测、校准或检验的报告或证书。

注：产品包装的判别标准是其可从产品上移除且不会导致产品分解、碎裂或损坏。附带信息的判别标准是其可分开获得或易于分离。型号标签或铭牌被视为产品的一部分。

7.4 本公司通过认证合同、公开文件、《认证注册通知书》要求客户组织做到：

1）在传播媒介（如互联网、宣传册或广告）或其他文件中引用认证标志时，应符合《认证注册通知书》的要求；

2）不做出或不允许有关于其认证资格的误导性的说明；

3）不以或不允许以误导性方式使用认证文件或其任何部分；

4）在其认证被暂停或撤销时，按照本公司的要求立即停止使用所有引用认证资格的广告材料；

5）在认证范围被缩小时，应修改相关广告材料；

6）不允许在引用其管理体系认证资格时，暗示认证机构对产品（包括服务）或过程进行了认证；

7）不得暗示或在认证范围以外的产品（包括服务）或过程中使用认证标识；

8）在使用认证资格时，不得使 DNI 声誉受损，失去公众信任；

9）获证客户对服务认证标志的使用应满足公开文件中说明性的规定。

7.5 本公司将正确地控制其认证文件的所有权，对于认证状态的错误引用或认证文件、标志

或审核报告的误导性使用，将采取要求纠正或采取纠正措施、暂停认证、撤销认证、公告违规行为以及必要的法律维权。

8、获证客户的信息通报

获证客户应及时通报其重大投诉、国家监督检查结果、重大事故及获证客户变更的各种信息等。变更信息包括（但不限于）以下：

1） 组织名称、组织法人、联系人、联系方式(包括：电话、邮箱、手机)等；

2） 组织地址(包括：注册地址、经营地址)；

3） 体系覆盖人数；

4） 认证范围变化；

5） 组织认证场所/服务点的增加；

6） 适用性声明及其版本的变化（信息安全管理体系适用）；

7） 业务、地点、组织结构和职能分配变化等情况的信息（及时通报）；

8） 认证客户的体系文件、信息的变化；

9） 有严重信息安全（包括已经或可能严重损害国家安全、社会秩序、公共利益或获证客户及其相关方的合法权益）的信息（及时通报）；

10）其他重要信息。（视情况）

当上述信息发生变更时，获证客户应填写《认证信息变更确认单》，并及时反馈给DNI。

特别注意：监督审核前，须主动与企业确认上述变化信息。

9、认证要求变更的条件和程序

9.1认证要求变更的条件

1） 获证客户保持认证资格有效；

2） 认证要求变更应在规定的时间前完成；

3） 申请认证要求变更的获证客户应提交认证要求变更需求申请，并提交按新的认证要求进行体系调整的证据；

4） 获证客户的管理体系已满足新的认证要求,且已正常运行。

9.2 认证要求变更的程序

1） 在认证要求变更转换期结束前，获证客户向DNI提出认证要求变更申请；提出申请日期宜在转换期截止前至少90天；

2） DNI通过对获证客户实施年度监督审核或再认证审核，或应获证客户要求安排的认证要求变更的专项审核，评审调整后的管理体系对认证要求的符合性、适宜性和有效性；

3） 经DNI审定，认为获证客户已满足批准认证资格的条件，同意批准认证范围，换发

认证证书或附件，认证证书的注册号和有效期保持不变。

10、保密

DNI承诺为认证客户保密（提前告知认证客户的需公开信息除外）。对认证客户的保密信息如需公开或向第三方提供时，将拟提供的信息提前通知认证客户（法律限制除外）。

如有证据表明，DNI因认证接触受审核方的商业、技术秘密，而泄露给第三者（法律规定除外），承担相应法律责任。

11、申诉/投诉、争议及处理

对DNI或审核人员违反国家认证法律、法规、机构有关规定、缺乏公正性及对认证的评价结果等有异议时，可以向DNI提出申诉、投诉，DNI将在30日内答复处理情况。

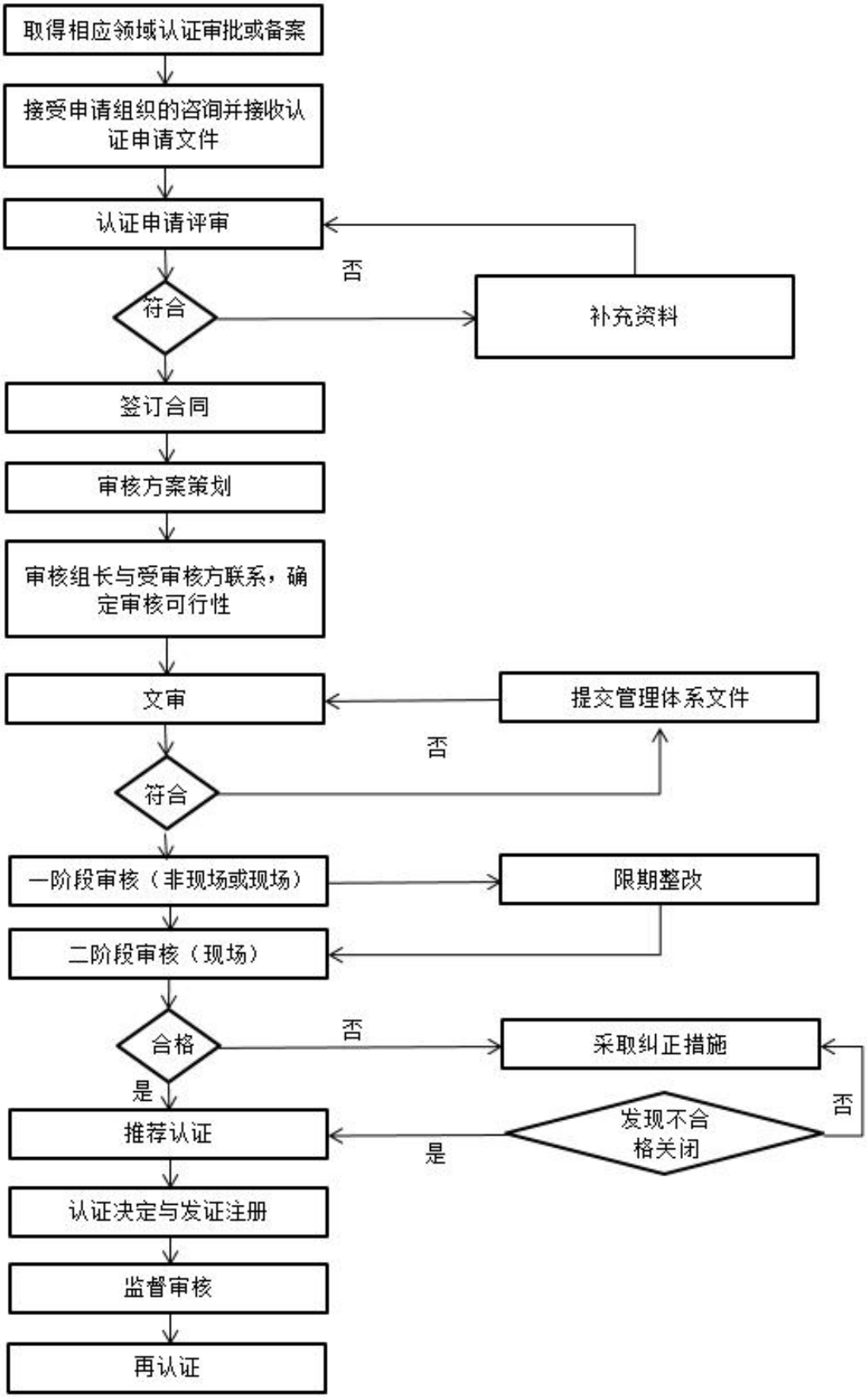
对DNI申诉/投诉和争议的处理有异议时可向有关部门进一步申诉/投诉。

参照《公开文件》中第七章：申诉、投诉和争议处理执行。

12、费用

实施本规则的费用，按公司发布的《公开文件》中第二章：认证收费标准执行。

附件一：管理体系认证业务流程图



附件二：认证业务范围表

大类	中类	级别	描述	备注
01	政务			
	01.01	一	国家机构	包括人大、政府、法院、检察院等，不含税务机关和海关
	01.02	一	税务机关	
	01.03	一	海关	
	01.04	二	其他	例如政党，政协，社会团体等
02			公共	
	02.01	一	通信、广播电视	
	02.02	一	新闻出版	包括互联网内容的提供
	02.03	二	科研	涉及特别重大项目的应提升为一级
	02.04	二	社会保障	例如社会保险基金管理、慈善团体等。包括医疗保险
	02.05	一	医疗服务	
	02.06	三	教育	
	02.07	二	其他	例如市政公用事业（水的生产和供应、污水处理、燃气生产和供应、热力生产和供应、城市水陆交通设施的维护管理等）
03			商务	
	03.01	一	金融	例如银行、证券、期货、保险、资产管理等
	03.02	一	电子商务	以在线交易为主要特点，含网络游戏
	03.03	一	物流	包括邮政
	03.04	三	咨询中介	例如法律、会计、审计、公证等
	03.05	二	旅游、宾馆、饭店	
	03.06	三	其他	
04			产品的生产	产品包括软件、硬件、流程性材料和服务
	04.01	一	电力	包括发电和输、变、配电等
	04.02	一	铁路	
	04.03	一	民航	
	04.04	一	化工	
	04.05	一	航空航天	
	04.06	一	水利	
	04.07	二	交通运输	包括公路、水路、城市公共客运交通等，不含航空和铁路
	04.08	二	信息与通信技术	例如软、硬件生产及其服务，系统集成及其服务，数字版权保护等
	04.09	二	冶金	
	04.10	二	采矿	含石油、天然气开采
	04.11	二	食品、药品、烟草	
	04.12	三	农、林、牧、副、渔业	
	04.13	三	其他	

附件三：ISMS体系有效人数与审核时间的关系表

在组织控制下工作的人员的数量	ISMS初次审核时间（审核人日）	在组织控制下工作的人员的数量	ISMS初次审核时间（审核人日）
1～10	5	876～1175	18.5
11～15	6	1176～1550	19.5
16～25	7	1551～2025	21
26～45	8.5	2026～2675	22
46～65	10	2676～3450	23
66～85	11	3451～4350	24
86～125	12	4351～5450	25
126～175	13	5451～6800	26
176～275	14	6801～8500	27
276～425	15	8501～10700	28
426～625	16.5	>10700	沿用以上规律
626～875	17.5		

附件四：认证证书样式


数网信认证
信息安全管理体系认证证书
注册号：XXXXXXXXXXXXXXX
兹证明
XXXXXXXXXXXXXXX 公司
统一社会信用代码：XXXXXXXXXXXXXXX
注册地址：XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
经营地址：XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
审核地址：XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
信息安全管理体系符合
ISO/IEC 27001:2022
通过认证范围：
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
颁证日期：xxxx 年 x 月 xx 日
有效期至：xxxx 年 x 月 xx 日
总经理：
日期：xxxx 年 x 月 xx 日
数网信认证服务（北京）有限公司
1. 本证书有效性查询可扫描二维码
2. 同时可登陆 www. swxrz. com 查询
3. 也可登陆国家认证认可监督管理委员会官方网站 www. cnca. gov. cn 查询
4. 获证组织必须定时接受监督审核并经审核合格此证书方继续有效
公众号
证书查询
数网信认证服务（北京）有限公司
认证机构地址：北京市朝阳区广渠路 36 号院 5 号楼 13 层 1327 电话：010-67723875 邮编：100020