编号：GK-MS-08-1/H

信息安全管理体系认证方案

发布日期：2025 年 8 月 20 日　　实施日期：2025 年 10 月 1 日

北京中大华远认证中心有限公司发布

目　录

信息安全管理体系认证方案

1 适用范围

本方案依据 GB/T 27007、GB/T 27021.1、GB/T 27060 的有关要求制定，规定了北京中大华远认证中心有限公司（以下简称 ZDHY）实施信息安全管理体系（以下简称 ISMS）认证的程序与管理的基本要求。必要时，ZDHY 在认证合同中补充相关认证要求。

信息安全管理体系可以开展的认证业务范围见附录 A。

2 认证依据

GB/T 22080-2025/ISO/IEC 27001:2022 《网络安全技术 信息安全管理体系 要求》

3 认证机构的基本要求

3.1 ZDHY 开展的认证活动围绕国家经济和社会发展目标，重点服务于经济社会高质量发展，不影响国家安全和社会公共利益，不违背社会公序良俗。

3.2 ZDHY 的内部管理和认证活动符合 GB/T 27021.1/ISO/IEC 17021-1《合格评定 管理体系审核认证机构要求 第 1 部分：要求》，以确保持续满足开展 ISMS 认证的基本要求。

3.3 ZDHY 对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：不将申请认证的组织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。

3.4 ZDHY 对认证活动中所知悉的国家秘密、商业秘密负有保密义务。ZDHY 通过在法律上具有强制实施力的认证合同，确保在认证活动中所获得的信息在未经申请组织书面同意的情况下，不向第三方透漏（监管有要求的除外）。

4 认证人员的基本要求

4.1 认证人员应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 认证审核员应取得国家认证认可监督管理委员会（以下简称“国家认监委”）确定的认证人员注册机构（CCAA）批准的信息安全管理体系审核员资格。

4.3 认证人员不得发生影响认证公正性的行为，应主动告知 ZDHY 他们所了解的任何可能使其或 ZDHY 陷入利益冲突的情况。

4.4 认证人员应按照 CCAA 要求接受人员注册/保持注册所要求的继续教育培训以及 ZDHY 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。

4.5 ZDHY 确保 ISMS 认证活动所涉及的各类认证人员满足以下要求：

（1）认证方案制定人员：具有 ISMS 认证知识，熟悉 ISMS 认证依据标准、认证程序以及有关法律法规、技术标准要求；

（2）认证申请评审人员：熟悉 ISMS 认证依据标准，能够正确判断认证申请信息的符合性；

（3）认证审核方案管理人员：熟悉 ISMS 认证依据标准、认证程序要求，能够根据认证申请组织的业务/产品/过程/组织结构的知识和信息完成审核方案和审核策划；

（4）认证审核人员：具有 ISMS 认证知识，理解和掌握 ISMS 认证依据标准，熟悉 ISMS 认证相关法律法规、审核原则、程序和方法，了解受审核组织业务管理的实践知识，ISMS 认证过程的管理要求，能够按照 ZDHY 的程序和过程开展工作；

（5）认证决定或复核人员：具有 ISMS 认证知识，熟悉认证认可相关标准及认证审核原则、实践和技巧，了解 ZDHY 认证管理过程要求；

（6）认证人员能力的评价人员：熟悉 ISMS 认证流程及认证过程各阶段的人员能力管理要求；熟悉各类认证人员的能力准则，能够正确选择对认证人员能力评价的方法，能够基于已有的证据准确判定受评价人员的能力与准则的符合性。

5 认证程序

5.1 认证申请

5.1.1 ZDHY 向申请认证的组织公开以下信息：

（1）ISMS 可以开展的认证业务的范围（见附录 A）；

（2）ISMS 认证方案（见本文件），包括：

a）开展 ISMS 认证活动所依据的认证标准或其他规范性要求；

b）认证方案和认证流程；

c）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规定；

d）拟向组织获取的信息以及保密规定；

e）认证收费标准；

f）认证证书、认证标志及相关的使用规定；

g）对认证过程和结果的申诉、投诉规定；

h）其他需要公开的信息。

5.1.2 提出认证申请时，申请组织应具备以下基本条件：

（1）申请组织和拟受审核组织应具有明确的法律地位，取得国家、地方市场监督管理

部门或有关机构注册登记的法人资格（或其组成部分），如工商营业执照、事业单位法人证书或社会团体法人登记证书等；

（2）申请组织和拟受审核组织应具有适用法律法规要求的经营/许可资质文件或强制性认证证书并保持有效；

（3）申请组织和拟受审核组织未被行政监管部门责令停业整顿，未被列入国家企业信用信息公示系统发布的严重违法失信名单；

（4）近一年内，拟受审核组织未发生重大网络安全事件；

（5）近一年内，拟受审核组织未受到政府主管部门行政处罚；

（6）近一年内，拟受审核组织未因自身原因被原发证机构暂停、撤销 ISMS 认证证书（适用时）；

（7）申请组织和拟受审核组织承诺始终遵守适用法律法规要求和 ZDHY 的认证要求；

（8）拟受审核组织已按照认证依据要求，建立并实施了文件化的 ISMS 且有效运行满 3 个月，至少已实施了一次完整的内部审核和管理评审；

（9）按照工信部联协[2010]394 号文《关于加强信息安全管理体系认证安全管理的通知》的要求，以及有关主管部门/监管部门对 ISMS 认证的管理要求，ZDHY 不受理各级政府机关和政府信息系统运营单位、涉密信息系统建设使用单位的 ISMS 认证申请；

（10）为政府部门提供信息技术外包服务的机构申请 ISMS 认证时，须经工业和信息化主管部门同意。通信、金融、铁路、民航、电力等基础信息网络和重要信息系统运营单位申请 ISMS 认证时，须经行业主管部门同意，涉及国计民生的国有企业申请 ISMS 认证时，须经国有资产监督管理部门同意，涉及国家秘密的应经保密行政管理部门同意。

5.1.3 申请组织应向ZDHY提交认证申请表及以下申请资料：

（1）对申请ISMS认证范围涉及的业务活动的描述，包括组织采用影响符合性的外包过程及相关内外部的接口关系说明；

（2）申请组织和拟受审核组织的法律地位证明文件（如企业营业执照、事业单位法人代码证书、社团法人登记证、非企业法人登记证书等）的复印件；当ISMS覆盖多个法律实体时，应提供每个法律实体的法律地位证明文件的复印件；

（3）申请认证范围所涉及的适用法律法规要求的行政许可文件、资质证书、强制性产品认证证书等证明文件的复印件；

（4）拟受审核组织的组织机构图、有关职责和权限的规定；

（5）可能影响认证过程适宜性和有效性的说明，包括：

a）申请组织的一般特征和相关信息，包括其名称、场所（包括临时场所）的地址、涉及虚拟场所和出于安保和安全问题不能公开物理位置的情况说明及其支持理由、过程和运作的重要方面（包括采用轮班作业）、人力资源和技术资源、职能和关系（适用时，包括其在一个较大实体中的职能和关系）；

b）寻求认证的其他标准或要求；

c）认证范围内不允许 ZDHY 接触的信息资产，或者 ZDHY 在接触相关信息资产时应满足的要求，包括法律法规、相关方和组织自身的要求；

d）认证范围内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进行核查的任何文件或记录；

e）申请组织寻求 ISMS 认证的其他标准或要求，包括向 ZDHY 说明适用的关于认证机构的资质、诚信守法记录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，并及时更新该说明；

f）所采用的所有影响符合性的外包过程；

g）接受与认证有关的咨询的情况；

（6）申请组织应向中心说明适用的关于 ISMS 认证机构的资质、诚信守法记录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，并即时更新该说明，以便中心判断其是否具备对该申请组织实施认证活动的资格或条件；

（7）申请组织应识别并向 ZDHY 告知其 ISMS 范围内的哪些信息资产不允许中心接触，或者 ZDHY 在接触相关信息资产时应满足哪些要求，包括法律要求、相关方的要求、需要通过 ISMS 应对的要求和组织自身的要求，ZDHY 应满足所有这些要求，否则不应在认证活动中接触申请组织的相关信息资产；

（8）申请组织是否存在因包含保密性或敏感性信息而导致不能提供给审核组核查的任何 ISMS 文件或记录（例如 ISMS 记录或关于控制的设计与有效性的信息），以便 ZDHY 确定 ISMS 是否能在缺少这些文件或记录的情况下得到充分审核。如果某些文件或记录对于审核来说是必需的且无法获取到时，那么只有在适当的访问安排获得许可后才能实施审核，或者采取相应的措施，例如终止审核、缩小审核和认证范围等；

（9）其他需要的申请资料。

申请组织应对认证申请表及相关申请资料的真实性和完整性负责。

5.2 申请评审

5.2.1 ZDHY对申请组织提交的认证申请表及有关申请资料进行评审，确保认证过程所需的

申请信息充分并与申请组织达成一致。评审内容包括：组织资质的合法性以及与申请基本条件的符合性，申请资料的完整性、适用性和有效性，ZDHY是否具备实施认证所需的能力。需要时，ZDHY通知申请组织对认证申请表及有关申请资料进行补充和完善。

5.2.2 满足以下条件的，ZDHY受理认证申请：

（1）认证申请组织和拟受审核组织已具备受理条件（见5.1.2）；

（2）ZDHY具备实施认证的能力；

（3）双方就认证事宜达成一致。

5.2.3 对于新的认证申请组织，ZDHY按照初次认证开展ISMS认证活动，无论其是否持有其他认证机构颁发的ISMS有效证书。

5.2.4 ZDHY将申请评审结果告知申请组织。ZDHY经评审，拒绝认证申请时，将告知申请组织被拒绝的原因。当认证申请对公正性产生威胁，或申请组织、拟受审核组织被列入国家企业信用信息公示系统发布的严重违法失信名单时，ZDHY不受理认证申请并告知申请组织。

5.3 认证合同

5.3.1 通过申请评审的，ZDHY将与申请组织签订具有法律效力的认证合同，以明确认证申请组织和ZDHY的责任。

5.3.2 ZDHY将及时向符合认证要求并已缴纳认证费用的组织颁发认证证书，通过国家认监委“全国认证认可信息公共服务平台”和ZDHY网站（www.zdhy.net）向社会公布获证信息。ZDHY将对获证组织ISMS的运行情况进行有效监督，发现获证组织的ISMS不能持续符合认证要求的，将及时暂停或者撤销其认证证书。

5.3.3 获证组织应承诺并履行以下责任：

（1）遵守ZDHY认证程序要求，认证过程如实提供相关材料和信息，通过ISMS认证后持续有效运行ISMS；

（2）配合认证监管部门的监督检查、配合ZDHY对投诉的调查；

（3）在广告、宣传等活动中正确使用认证证书、认证标志和有关信息，认证证书注销或被暂停、撤销的，不得继续使用该证书和相关认证标志、信息；

（4）及时向ZDHY通报ISMS的重大变更和其他已经或可能导致ISMS不能满足认证要求的严重情况；

（5）按照认证合同约定及时向ZDHY缴纳认证费用。

5.4 审核方案和审核策划

5.4.1 审核方案

5.4.1.1 ZDHY针对每一申请组织建立认证周期内的审核方案，以清晰识别所需的审核活动。

5.4.1.2 初次认证的审核方案包括两个阶段的初次审核、获证后的监督审核和认证到期前的再认证审核。

5.4.1.3 初次认证审核和再认证审核是对受审核组织完整体系的审核，应覆盖认证依据所有的适用要求。认证周期内的全部审核应覆盖认证依据所有的适用要求。

5.4.1.4 初次认证后的第一次监督审核应在认证证书签发之日起12个月内进行，第二次及以后的监督审核的时间间隔自上次监督审核日期起不超过12个月。

5.4.1.5 ZDHY基于受审核组织不同班次的过程和活动以及所证实的每个班次的ISMS控制水平，策划对不同班次实施的审核程度，确保审核的有效性。每次审核至少对其中一个班次的过程和活动现场进行审核。

5.4.2 审核时间

5.4.2.1 审核时间包括在受审核组织现场的审核时间以及在现场审核以外的实施策划、文件评审和编写审核报告等活动的时间。审核时间以人日计算，1人日为8小时。如果每天的实际工作时间不足8小时，则可以延长审核天数以满足人日要求。

5.4.2.2 本方案附录B明确了ISMS审核时间要求。ZDHY以附录B确定的审核时间为基础，考虑受审核组织的规模和性质、所在行业特点、认证范围覆盖的场所数量、管理过程和活动的复杂程度、所使用的审核方法和语言、后勤条件等因素，确定策划和完成一个完整有效的审核所需的审核时间。当ZDHY基于上述因素减少审核时间时，减少的时间不超过附录B所规定的审核时间的30%。现场审核时间不少于所确定的审核时间的80%。

5.4.2.3 当ISMS与其他管理体系实施结合审核时，ZDHY将分别确定每个管理体系所需的审核时间，结合审核的总审核时间不少于每个管理体系所需审核时间之和的80%。

5.4.2.4 ZDHY 提前与受审核组织就现场审核日期和持续时间沟通并达成一致，向受审核组织下达审核通知。进入现场审核前，受审核组织如对现场审核信息存有异议（包括任何更改），应及时向 ZDHY 反馈。ZDHY 确认需要变更现场审核信息时，就变更信息与受审核组织达成一致，重新下达审核通知。

5.4.3 多场所抽样方案

5.4.3.1 多场所受审核组织可以包含一个以上的法律实体，但该组织的所有场所应与组织的中心职能具有法律或合同联系，并服从于单一的管理体系。该管理体系应由中心职能制定、

建立，并服从于中心职能的持续监督和内部审核。

5.4.3.2 当多场所组织的多个场所均实施非常相似的过程、活动时，ZDHY可对其进行抽样审核。样本应选择有代表性的不同场所，确保覆盖认证范围内的所有过程和活动。ZDHY将基于各场所规模上的显著差异、不同场所管理过程和活动的复杂程度、以往审核的结果、上次审核后的变化、法律法规方面的差异、地理位置的分散程度等因素来选择场所。

5.4.3.3 ZDHY 通过申请评审来确定多场所项目中拟实施现场审核的场所，形成抽样计划并记录其合理性。对多个相似场所进行抽样审核时，每次审核最少访问的场所数量是：

（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：y 为抽样数量，计算结果向上取整；x 为相似场所的总体数量。

初次认证审核、监督审核以及再认证审核时都应对中心职能进行审核。

5.4.3.4 对于多场所项目，ZDHY 按照附录 B 确定每个场所的审核时间。当某些过程不适用于某个场所时（如某过程的管理职责属于对其进行控制的具有中心职能的场所），可以减少该场所的审核时间。现场审核时间不得少于依据附录 B 所确定的现场审核时间的 50%。

5.4.4 组建审核组

5.4.4.1 ZDHY 根据实现审核目的所需的能力和公正性要求组建审核组。审核组应满足以下要求：

（1）组内的审核员应具备CCAA批准的信息安全管理体系审核员资格，经ZDHY能力评价合格；

（2）ZDHY 指定组内的一名审核员担任审核组长，审核组长应具有管理和领导审核组达成审核目标的知识和技能，其能力应至少满足 GB/T 19011《管理体系审核指南》标准中对审核组长的通用要求；如果审核组仅有一名审核员，则该审核员应具备履行审核组长职责的能力；

（3）组内至少有一名与拟受审核组织所属认证业务范围相匹配的 ISMS 专业人员（专业审核员或技术专家）；

（4）组内审核员所需的知识和技能可以通过技术专家和（或）翻译人员进行补充，技术专家和（或）翻译人员应在审核员的指导下工作，其选择应避免他们对审核产生不当影响；

（5）技术专家主要负责为审核组提供技术支持，不作为审核员实施审核，不计入审核时间；

（6）实习审核员应在正式审核员的指导下参加审核，不计入审核时间，其在审核过程中的活动由负责指导的正式审核员承担责任，组内实习审核员的数量不得超过正式审核员的数量；

（7）当 ISMS 与其他管理体系结合审核时，审核组还应满足其他管理体系认证方案中有关组建审核组的要求。

5.4.4.2 审核组成员不得与受审核组织存在利益关系。

5.4.5 审核计划

5.4.5.1 审核组长依据审核方案为每次现场审核制定审核计划。审核计划至少包括审核目的、审核依据、审核范围、现场审核日期、时间安排和场所、审核组成员及审核任务安排。现场审核应安排在受审核组织 ISMS 范围内的管理过程和活动处于正常运行时进行。

5.4.5.2 现场审核开始之前，审核组长将审核计划提交给受审核组织确认。如需要临时调整审核计划，审核组长应及时与受审核组织沟通，变更后的审核计划经双方协商一致后实施。

5.5 实施审核

5.5.1 审核组长领导审核组全员，按照审核计划实施现场审核。审核组应按照国家认监委的要求完成首、末次会议现场审核的网络签到。

5.5.2 审核组与受审核组织管理层（适用时，还包括拟审核区域或过程的负责人员）召开首次会议，向受审核组织介绍审核组成员及其角色，说明审核安排并解释审核活动和方式，确认受审核组织同意审核计划安排以及所策划的审核活动能够实施。

5.5.3 现场审核过程中，审核组采用面谈、观察过程和活动、审查文件和记录以及其他适用的审核方法，通过适当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）并加以验证使之成为审核证据。审核组对照审核准则评价审核证据以确定审核发现，包括关于不符合的审核发现。

5.5.4 现场审核期间，审核组长应及时向受审核组织沟通进度、重要审核发现和任何关注，解决与审核证据或审核发现有关的任何分歧。当获得的审核证据表明不能达到审核目的时，审核组长应向受审核组织、申请组织和ZDHY报告理由以确定适当的措施。这些措施可以包括审核策划、审核目的或审核范围的变更或终止审核。发生下列情况时，审核组应向ZDHY报告，经ZDHY同意后终止审核：

（1）受审核组织对审核活动不予配合，导致审核活动无法进行；

（2）受审核组织实际情况与申请信息有重大不一致；

（3）其他导致审核程序无法完成的情况。

5.5.5 审核组应与受审核组织确认不符合事实及其分级（轻微不符合与严重不符合），确保审核证据准确且不符合得到理解，同时就审核结论、必要的跟踪活动和所需要的修改达成一致。

5.5.6 审核组与受审核组织的管理层（适用时，还包括拟审核区域或过程的负责人员）召开末次会议，提出审核发现和审核结论（包括关于认证的推荐性意见），并就不符合的纠正和纠正措施的验证方式与期限达成一致。

5.5.7 审核组按照审核计划完成所有的现场审核活动，向 ZDHY 提交审核报告，按照以下类型给出现场审核结论的建议：

（1）现场审核通过：现场审核全部符合要求，未发现不符合；

（2）书面验证通过：现场审核发现不符合，受审核组织已在规定期限内提交了为消除不符合已采取或拟采取的具体纠正和纠正措施证据，经审核组书面验证可接受；

（3）现场验证通过：现场审核发现不符合，受审核组织已在规定期限内提交了为消除不符合已采取或拟采取的具体纠正和纠正措施证据，经审核组现场验证可接受。

逾期未能完成纠正和纠正措施的验证或经验证不可接受的，现场审核结论为未通过。

5.6 初次认证

5.6.1 第一阶段审核

5.6.1.1 第一阶段审核目的是通过了解受审核组织的ISMS及其对第二阶段审核的准备情况，确定受审核组织是否具备接受第二阶段审核的条件并策划第二阶段审核的关注点。第一阶段审核的内容包括但不限于以下方面：

（1）了解受审核组织的情况，包括其活动、产品和服务设施设备、生产和（或）服务提供流程、现场运作以及适用的法律法规、标准和其他规范性要求；

（2）评审受审核组织的ISMS文件，确认文件内容与组织业务活动及产品和服务吻合；

（3）审核受审核组织理解和实施认证依据的情况，特别是对ISMS关键绩效、过程和运行及管理目标识别情况；

（4）受审核组织是否为第二阶段审核做好准备，已实施了内部审核和管理评审；

（5）确认受审核组织ISMS认证范围、体系覆盖范围内的有效人数和场所；

（6）受审核组织的产品和服务符合相关法律法规及强性标准的情况。

5.6.1.2 第一阶段审核包括文件评审和现场访问。

对于文件评审，审核组长应在现场审核前审查审核组织的ISMS文件，确定与认证依据的符合性，并获取受审核组织对ISMS进行有效策划的信息。审核组长经评审，确认审核组织ISMS文件符合认证依据，文件评审通过。审核组长将文件初审意见告知受审核组织，包括识别任何引起关注的、可能被判定为不符合的问题。对于文件评审中发现的不修改则会影响现场审核的问题，受审核组织应在规定期限内完成修改，审核组长再次审查并接受后，文件评审通过。

对于现场访问，审核组长应编制第一阶段审核计划，在现场访问前提交给受审核组织确认。现场访问过程中，审核组长应领导审核组成员，通过与受审核组织各层级人员的交谈以及

走访受审核组织ISMS的主要运行场所，了解受审核组织ISMS及其方针、目标、风险、过程和现场运行情况，为第二阶段审核收集必要的信息。

5.6.1.3 审核组与受审核组织管理层进行沟通，将第一阶段审核目的是否实现、第二阶段审核是否准备就绪以及第一阶段审核发现以书面形式告知受审核组织，包括所识别的任何应引起关注的、在第二阶段审核可能被判定为不符合的问题。

第一阶段审核提出的需要在第二阶段审核前完成纠正的问题，审核组长经验证并确认得到解决之后，方可实施第二阶段审核。

受审核组织存在ISMS文件与现场实际情况不符，审核范围覆盖的管理活动和过程未正常开展和运行，ISMS运行不足3个月或无法证明已满3个月，以及其他不具备现场审核条件的情形时，ZDHY不能实施第二阶段审核。

如果受审核组织发生任何影响其ISMS的重大变更，ZDHY将考虑重复整个或部分第一阶段审核。

第一阶段审核结果可能导致推迟或取消第二阶段审核。

5.6.2 第二阶段审核

5.6.2.1 第二阶段审核目的是评价受审核组织ISMS的实施情况，包括对认证依据的符合性和体系的有效性。

5.6.2.2 第二阶段审核应在受审核组织现场进行，至少覆盖以下审核内容：

（1）受审核组织ISMS文件化信息的符合性和适宜性；

（2）受审核组织ISMS范围、场所、过程和活动的必要信息，ISMS与认证依据或其他规范性文件的所有要求的符合情况及证据；

（3）受审核组织ISMS方针和目标的实现程度；

（4）受审核组织依据其确定的 ISMS 关键绩效和目标，对绩效进行的监视、测量、报告和评审的情况；

（5）受审核组织 ISMS 实现其预期结果的能力，以及在符合适用法律法规要求和合同要求方面的绩效；

（6）受审核组织 ISMS 过程的运行控制情况；

（7）受审核组织策划并实施 ISMS 内部审核和管理评审的有效性；

（8）确认适用的法律地位文件、生产经营许可证书、资质证书、强制性产品认证证书等证明文件的有效性。

5.7 监督审核

5.7.1 ZDHY 采用日常监督活动与监督审核相结合的方式，对获证组织进行有效跟踪，以确认

获证组织 ISMS 与认证依据要求的持续符合性和运行的有效性。

5.7.2 日常监督活动

ZDHY 实施日常监督活动包括：

（1）评审获证组织向 ZDHY 通报的信息；

（2）ZDHY 就认证的有关方面询问获证组织；

（3）审查获证组织对其运作的说明（如宣传材料、网页）；

（4）要求获证组织提供有关的文件化信息（纸质或电子介质）；

（5）其他监视获证组织绩效的方法（如关注国家有关部门发布的信息等）。

5.7.3 监督审核

5.7.3.1 初次认证后的第一次监督审核应在认证证书签发之日起 12 个月内进行，第二次及以后的监督审核的时间间隔自上次监督审核日期起不超过 12 个月。发生以下情形时，ZDHY 将考虑增加监督审核频次或单独实施一次专门的审核（即专项审核）：

（1）获证组织 ISMS 发生重大变更时，包括法人、场所、设施、组织机构、有关职能、资源、产品和服务、过程等影响其认证基础的变更；

（2）认证依据发生变化时；

（3）对被暂停认证资格的获证组织进行追踪；

（4）获证组织出现相关方提出对 ISMS 运行效果的投诉未做出任何回应时；

（5）发生其他影响符合认证要求的能力变化的特殊情况时；

（6）其他需要考虑的情况。

5.7.3.2 ZDHY 对监督审核进行策划，以便对获证组织 ISMS 范围内有代表性的区域和职能进行监视。监督审核在受审核组织现场进行，重点关注获证组织的变更以及 ISMS 绩效的持续改进，监督审核内容至少包括：

（1）审查与认证覆盖范围相关的法律地位文件、生产经营许可证书、资质证书、强制性产品认证证书等证明文件的有效性；

（2）获证组织 ISMS 的任何变更；

（3）获证组织 ISMS 在实现其目标和预期结果方面的有效性；

（4）获证组织 ISMS 持续的运作情况及其有效性，包括对适用法律法规和其他规范性要求的识别和遵守情况；

（5）获证组织策划和实施 ISMS 内部审核和管理评审的有效性；

（6）获证组织为持续改进其 ISMS 所策划的活动的进展和效果；

（7）获证组织对 ISMS 相关投诉的处理，以及投诉对保持认证的影响；

（8）适用时，获证组织对上次审核确定的不符合所采取的纠正措施的有效性；

（9）获证组织对认证证书、认证标志的使用和（或）任何其他对认证信息的引用。

5.7.4 ZDHY 基于获证组织 ISMS 的成熟度和稳定性、管理过程和活动特点、所承担的风险等因素，合理确定监督审核的时间间隔和频次。监督审核一般为现场审核，ZDHY 按照本方案 5.4、5.5 的要求策划并实施监督审核。当获证组织的 ISMS、管理体系文件发生重大变更，可能影响其与认证依据要求的符合性时，ZDHY 将针对变更实施文件评审。

5.8 再认证

5.8.1 获证组织拟继续持有认证证书的，应在认证证书有效期满前 4 个月内，按照本方案 5.1 的要求向 ZDHY 提出再认证申请。ZDHY 按照本方案 5.2、5.3 的要求实施申请评审，经评审同意受理再认证申请时，与申请组织签订具有法律效力的认证合同。

5.8.2 ZDHY 依据审核方案实施再认证审核，以判断获证组织的 ISMS 作为一个整体与认证依据要求的持续符合性和运行的有效性。再认证审核内容至少包括：

（1）审查与认证覆盖范围相关的法律地位文件、生产经营许可证书、资质证书、强制性产品认证证书等证明文件的有效性；

（2）结合内外部环境的变化情况，确认获证组织 ISMS 的持续有效性以及认证范围的持续相关性和适宜性；

（3）获证组织 ISMS 持续的运行控制情况，以及在实现其目标和预期结果方面的有效性，包括对适用法律法规和其他规范性要求的识别和遵守情况；

（4）适用时，获证组织对上次审核确定的不符合所采取的纠正措施的有效性；

（5）获证组织对认证证书、认证标志的使用和（或）任何其他对认证信息的引用；

（6）获证组织在上一个认证周期内的绩效，保持 ISMS 有效性并实现改进以提高整体绩效的情况及其效果。

5.8.3 ZDHY 按照本方案 5.4 的要求实施再认证审核策划，策划将考虑获证组织最近一个周期内的 ISMS 绩效，包括调阅以往的监督审核报告。再认证通常包括文件评审和现场审核，文件评审按照本方案 5.6.1.2 的要求实施，现场审核按照本方案 5.4、5.5 的要求实施。

5.8.4 当获证组织发生影响认证有效性的重大变更，或 ZDHY 对相关投诉的分析，或 ZDHY 通过日常监督活动和监督审核获取的信息表明获证组织不再满足认证要求时，ZDHY 将提前对获证组织实施再认证。

5.8.5 获证组织在认证证书被暂停使用期间提出再认证申请，ZDHY 执行认证恢复及再认证程序。

5.8.6 上一周期认证证书到期后，如果 ZDHY 能够在 6 个月内完成未尽的再认证活动，则可以恢复认证，否则应至少进行一次第二阶段审核才能恢复认证。新一周期认证证书的生效日期不应早于再认证决定日期，终止日期应基于上一个认证周期。

5.8.7 上一周期认证证书到期后，如果 ZDHY 未能在 6 个月内完成未尽的再认证活动，则获证组织上一周期认证证书到期后即失效。获证组织应重新提出认证申请，ZDHY 执行初次认证程序。

5.9 特殊审核

对于已授予的认证，获证组织提出扩大认证范围的申请时，ZDHY 将对该申请进行评审，并确定任何必要的审核活动，以做出是否予以扩大认证范围的决定。这类审核活动可以结合监督审核同时进行。

5.10 不符合及其验证

5.10.1 审核中发现的不符合项分为轻微不符合项和严重不符合项，审核组将形成书面不符合报告。受审核组织应在规定时限内分析原因，策划和实施为消除不符合及其原因已采取或拟采取的具体纠正和纠正措施，向审核组提交相关证据。审核组对受审核组织所采取的纠正和纠正措施的有效性进行验证。

审核组应在末次会议上规定不符合项的整改时限（通常自末次会议结束之日起 1 个月内，最长不超过 6 个月）以及纠正和纠正措施有效性的验证方式（书面验证或现场验证）。

如果受审核组织未能在规定的时限内采取适当的纠正和纠正措施并经审核组长验证有效，ZDHY 不能做出授予认证、保持认证或更新认证的决定。

5.10.2 对于轻微不符合项，受审核组织可以制定纠正措施计划，ZDHY 在下次审核时审查纠正措施的实施情况并验证其有效性。

5.10.3 对于初次认证审核确定的严重不符合项，受审核组织应在第二阶段审核结束之日起 6 个月内采取适当的纠正和纠正措施并经审核组验证有效，否则审核组不能向中心推荐认证注册，或 ZDHY 再实施一次第二阶段审核。

5.10.4 对于监督审核确定的严重不符合项，获证组织应在审核结束之日起 3 个月内采取适当的纠正和纠正措施并经审核组验证有效，否则审核组不能向中心推荐保持认证。

5.10.5 对于再认证审核确定的严重不符合项，获证组织应在原认证证书到期前采取适当的纠正和纠正措施并经审核组验证有效，否则获证组织上一周期认证证书到期后即失效。

5.11 审核报告

5.11.1 ZDHY就每次审核向申请组织提供书面的审核报告。ZDHY享有审核报告的所有权。

5.11.2 审核组长编写审核报告，审核报告的内容应准确、简明和清晰，以便为认证决定提供充分的信息。审核报告包括或引用以下内容：

（1）ZDHY 名称；

（2）申请组织名称，受审核组织的名称、地址及其代表；

（3）审核类型（如初次审核、监督审核、再认证或其他类型审核）和审核方式（适用时，结合、联合或一体化审核情况）；

（4）审核目的、准则、范围以及审核时间；

（5）审核组成员姓名、组内职务以及任何与审核组同行的人员；

（6）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；

（7）主要审核路线和所使用的审核方法的说明，包括文件评审的摘要，运行控制场所的抽样及样本信息；

（8）与审核类型要求相一致的审核发现、审核证据（或审核证据的引用）以及审核结论（包括审核组的推荐性意见），有关认证要求符合性的陈述（包括任何不符合项），受审核组织实际情况与其预期管理目标之间存在的差距和改进机会；

（9）任何偏离审核计划的情况及其理由；

（10）已识别出的任何未解决的问题；

（11）任何影响审核方案的重要事项；

（12）适用时，上次审核后发生的影响受审核组织 ISMS 的重要变更；

（13）适用时，不符合项纠正措施的有效性验证情况；

（14）适用时，获证组织使用认证证书、认证标志和（或）引用认证信息的符合性。

（15）说明审核基于对可获得信息的抽样过程的免责声明。

5.11.3 对终止审核的项目，审核组应将终止审核的原因以及已开展的审核情况形成报告，ZDHY将此报告提交给申请组织。

5.11.4 受审核组织应妥善保管审核报告、审核计划、不符合报告及纠正措施证据等文件化信息。

5.12 复核与认证决定

5.12.1 ZDHY 在对审核过程的相关资料、审核报告、不符合项纠正和纠正措施及验证情况以及其他信息进行复核与综合评价的基础上，做出认证决定。认证决定人员不得为审核组成员。

5.12.2 ZDHY 应有充分的证据确认申请组织满足下列条件时，做出授予、更新、扩大认证范围的决定：

（1）受审核组织满足本方案5.1.2所述的基本条件；

（2）对于严重不符合，已审查、接受并验证了受审核组织纠正措施的有效性；

（3）对于轻微不符合，已审查、接受了受审核组织的纠正措施或计划采取的纠正措施；

（4）受审核组织的ISMS总体符合认证依据要求且运行有效；

（5）认证申请组织按照认证合同规定履行了相关义务。

5.12.3 ZDHY对符合认证要求的申请组织颁发认证证书。对不符合认证要求的申请组织，ZDHY将告知其不能通过认证的原因。申请组织如要继续认证，需重新申请认证。

5.12.4 ZDHY基于监督审核的结果，确认获证组织持续满足认证要求时，做出保持认证的决定，向获证组织发出保持认证的通知。确认获证组织不能持续满足认证要求时，按照本方案7的要求做出相应处置。

5.12.5 对于再认证，ZDHY 在当前认证证书的终止日期前完成了再认证活动，确认获证组织持续满足认证要求时，做出授予认证证书的决定，为获证组织换发新一周期的认证证书，重新赋予认证证书编号和有效期。对于初次认证以来未中断的再认证证书，ZDHY 可在证书上表述获证组织初次获得证书的日期。原则上，新一周期认证证书的发证日期为再认证决定日期，有效期为 3 年。如果获证组织提出保持认证证书有效期连续状态的要求，则新一周期认证证书的终止日期也可以基于前一周期认证证书的终止日期。

上一周期认证证书到期后，如果 ZDHY 能够在 6 个月内完成再认证活动并做出授予认证证书的决定时，新一周期认证证书的发证日期为再认证决定日期，终止日期将基于上一周期认证证书的终止日期。

当确认获证组织不再满足认证要求时，ZDHY 做出不授予认证证书的决定。如果 ZDHY 在上一周期认证证书终止日期前未能完成再认证决定，则不应延长认证的效力，获证组织上一周期认证证书到期后即失效。

6 认证证书和认证标志

6.1 总则

6.1.1 获证组织可以在认证有效期内使用 ISMS 认证证书和认证标志，接受 ZDHY 的监督管理。ZDHY 拥有 ISMS 认证证书和认证标志的所有权，禁止任何组织和个人伪造、冒用、转让和非法买卖认证证书和认证标志。

6.1.2 获证组织应当在广告等有关宣传中正确使用 ISMS 认证证书和认证标志，不得将 ISMS 认证标志标注在产品或产品的包装、标签、铭牌上，或以任何其他可解释为产品符合性的方式

使用。获证组织可在产品包装（如运输包装）上或附带信息中声明获证组织的 ISMS 通过认证，但声明决不应暗示产品、过程或服务以这种方式得到了认证。

注 1：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。

注 2：型号标签或铭牌被视为产品的一部分。

获证组织不可将 ZDHY 的认证标志用在实验室检测、校准或检查的报告或证书上。

6.1.3 ZDHY 发现获证组织未正确使用认证证书和认证标志时，将要求获证组织立即采取有效纠正措施并跟踪监督纠正情况。

6.2 认证证书

6.2.1 ZDHY向认证决定符合要求的组织出具ISMS认证证书，认证证书的签发日期不早于做出认证决定的日期。

6.2.2 ISMS认证证书的有效期最长为3年，初次认证证书有效期的起算日期为认证决定日期。

6.2.3 ZDHY对每张ISMS认证证书赋予一个编号，认证证书编号规则见本方案附录C。

6.2.4 ISMS认证证书的信息应真实、准确，不产生误导，并包含以下内容：

（1）认证证书的名称和编号，认证标志和相关认可标识（适用时）；

（2）获证组织名称、注册地址和统一社会信用代码；

（3）认证范围所覆盖的经营地址。若认证的 ISMS 覆盖多场所时，将表述认证所覆盖的所有场所的地址信息；

（4）获证组织 ISMS 所覆盖的产品、活动、服务的范围；适用时，包括每个场所相应的认证范围，且没有误导或歧义；

（5）认证依据号；

（6）ZDHY 的名称和地址；

（7）认证证书的签发人、发证日期（即生效日期）和认证有效期或终止日期；

（8）证书信息及证书状态的查询途径；

（9）获证组织必须定期接受监督审核以保持认证证书的提示信息。

6.3 认证标志

获证组织可以在广告、宣传品中正确使用以下认证标志并保证其完整不变形。

6.4 认证证书的变更

6.4.1 认证证书有效期内，获证组织发生影响或可能影响 ISMS 与认证依据要求持续符合性和运行有效性的变更，应向 ZDHY 提出变更申请并提交有关申请资料，ZDHY 将对变更申请进行评审，确定任何必要的审核活动（如：文件评审，现场审核），以做出是否予以变更认证的决定。这类审核活动可以结合监督审核或再认证审核同时实施，也可以专项审核的形式单独实施。

变更的情形可能包括：

（1）获证组织名称、地址名称的更改；

（2）认证范围内，获证组织管理体系的过程或活动范围发生缩小（如部分过程和活动不再进行）、扩大（如增加了新的过程或活动）或其他变更（如改变了原有的过程或活动）；

（3）认证范围内，获证组织管理体系运行的场所发生缩小（如部分原场所不再使用）、扩大（如在原有场所地址上扩建、在其他地址上建设新场所等）或其他变更（如搬迁至新场所）；

（4）认证依据的变更；

（5）其他影响认证证书保持的变更。

6.4.2 ZDHY 经评审，确认变更未对获证组织认证证书的保持产生影响，或变更不需要通过现场审核进行确认时，将批准认证证书的变更，为获证组织换发新的认证证书。

6.4.3 ZDHY经评审，确认变更将对获证组织认证证书的保持产生影响，且需要通过现场审核确认时，ZDHY将按照本方案5.4、5.5的要求策划并实施现场审核。

ZDHY经现场审核，确认获证组织的变更符合认证要求时，做出变更认证证书的决定，为获证组织换发新认证证书。换发新认证证书后，原认证证书随即注销。

6.4.4 当变更涉及认证范围的扩大或重大变化（如改变了原有的运行场所、过程或活动）时，ZDHY将在现场审核前对变更部分实施文件评审，确定与认证依据要求的符合性。文件评审通过后，方可进入现场审核。

6.4.5 认证证书有效期内，因证书所覆盖的获证组织名称、地址、过程或活动范围、认证依据等变更而换发的新认证证书，其证书号和有效期截止日期不变。ZDHY 标注原认证证书的发证日期和换证日期，换证日期以换发新证书的批准日期为准。

6.4.6 认证证书变更后，获证组织应按照 ZDHY 要求正确使用变更后的认证证书，及时审查与认证信息相关的广告及宣传材料的内容，必要时对其做出修改。

7 认证资格的暂停、撤销和注销

7.1 总则

当获证组织违反ZDHY的有关认证规定或无法达到ZDHY的认证要求时，ZDHY将对获证组织的认证证书做出相应的暂停、撤销或注销处理，并公开处理结果。

7.2 认证资格的暂停

7.2.1 获证组织存在以下情形之一的，ZDHY 将在调查核实后暂停其认证资格（暂停期限最长不超过 6 个月）：

（1）违反 ZDHY 要求，不承担、履行认证合同约定的责任和义务，包括：

a）不能按照 ZDHY 规定的时间间隔接受监督活动（包括监督审核、跟踪调查）或再认证；

b）监督审核发现的严重不符合项未得到有效纠正，或发现的轻微不符合项未在规定期限内完成纠正措施；

c）未按照 ZDHY 的要求正确引用或宣传获得的认证资格和有关认证信息，包括认证证书和认证标志的使用，造成严重影响或后果；

d）未按照 ZDHY 的要求通报有关信息；

e）未按时缴纳认证相关费用；

f）不承担、履行认证合同约定的其他责任和义务；

（2）ISMS 持续或严重地不满足认证要求的；

（3）持有的与认证范围有关的行政许可文件、资质证书、强制性认证证书等过期失效；

（4）不满足认证范围适用的法律法规要求，且未采取有效纠正措施；

（5）受到与认证范围内的产品/服务相关的行政处罚；

（6）发生信息安全破坏事故，已经或可能严重损害国家安全、社会秩序、公共利益或获证组织及其相关方的合法权益；

（7）拒绝配合市场监管部门的认证执法监督检查，或者提供虚假材料或信息；

（8）被有关行政监管部门责令停业整顿；

（9）发生与认证范围内的管理过程或活动相关的重大舆情；

（10）主动请求暂停认证证书并经 ZDHY 同意；

（11）其他应暂停认证证书的情形。

7.2.2 认证证书有效期内，ZDHY通过对日常监督活动、监督审核结果以及获证组织相关方投诉信息的评审，确认获证组织存在应暂停认证证书的情形时，做出暂停其认证证书使用的决定并公开暂停信息。

被暂停使用认证证书的组织应按照 ZDHY 的要求，立即停止涉及认证信息的广告及宣传活动，不得以任何方式使用认证证书、认证标志或引用认证信息。认证证书被暂停使用期间，获证

组织的认证资格暂时无效。因获证组织违规宣传引起严重后果的，ZDHY将采取必要的法律手段。

需要时，获证组织可以主动向 ZDHY 申请暂停其持有的认证证书。

7.2.3 认证证书被暂停使用期间，组织应在规定期限内向ZDHY提出恢复申请并提交有关证据。ZDHY经评审，确认组织提交的证据能够证实其解决了造成暂停的问题，不需要实施现场审核的，将批准恢复认证证书的使用并公开恢复信息。

ZDHY经评审，确认需要实施现场审核的，将结合监督审核、专项审核或再认证审核进行。ZDHY根据现场审核结果，确认组织已在规定期限内解决了造成暂停的问题，做出恢复使用认证证书的决定并公开恢复信息。

7.3 认证资格的撤销

7.3.1 获证组织存在以下情形之一的，ZDHY 将在获得相关信息并确认后撤销其认证资格：

（1）不承担、履行认证合同约定的责任和义务的；

（2）被注销或撤销法律地位证明文件的；

（3）被行政监管部门认定存在严重违法失信行为，或被国家企业信用信息公示系统列入严重违法失信名单的；

（4）认证证书暂停使用后，未在规定期限内解决造成暂停的问题（包括持有的与认证范围有关的行政许可文件、资质证书、强制性认证证书等已经过期失效但换证申请未获批准）；

（5）因获证组织违规造成与认证范围有关的重大事故的；

（6）拒不接受相关行政监管部门或 ZDHY 对其实施的监督活动，或对有关事项的询问和调查提供了虚假材料或信息的；

（7）存在其他严重违反认证范围适用的法律法规的行为，受到相关行政监管部门处罚的；

（8）管理体系未运行或已不具备运行条件的；

（9）未按照 ZDHY 要求正确引用和宣传认证信息，造成严重影响或后果，或 ZDHY 已要求其纠正但超过 1 个月仍未纠正的；

（10）在认证过程中存在隐瞒真实情况、弄虚作假行为，严重影响认证有效性的；

（11）发生重大网络安全事件，已经或可能严重损害国家安全、社会秩序、公共利益或获证组织及其相关方的合法权益；

（12）其他应撤销认证资格的情形。

7.3.2 认证证书有效期内，ZDHY 通过对日常监督活动、监督审核结果以及获证组织相关方投诉信息的评审，确认获证组织存在应撤销认证证书的情形时，做出撤销其认证证书的决定并公开撤销信息。

被撤销认证证书的组织应按照ZDHY的要求，立即停止使用被撤销的认证证书和认证标志，以及任何其他对被撤销认证资格的引用。组织应立即停止涉及认证信息的广告及宣传活动。因获证组织违规宣传引起严重后果的，ZDHY将采取必要的法律手段。

7.4 认证资格的注销

7.4.1 存在以下情形之一时，ZDHY将注销获证组织的认证资格：

（1）获证组织主动申请注销认证证书；

（2）获证组织的认证证书有效期届满，未申请延续使用；

（3）ZDHY换发新认证证书时，将注销旧认证证书；

（4）其他需要注销认证证书的情形。

7.4.2 ZDHY确认获证组织存在应注销认证证书的情形时，做出注销其认证证书的决定并公开注销信息。被注销认证证书的组织应按照ZDHY的要求，立即停止使用被注销的认证证书和认证标志，以及任何其他对被注销认证资格的引用。组织应立即停止涉及认证信息的广告及宣传活动，因获证组织违规宣传而引起严重后果的，ZDHY将采取必要的法律手段。

8 申诉（投诉）处理

8.1 申请组织或获证组织对认证决定有异议的，可以向ZDHY提出申诉。任何组织和个人对认证过程和决定有异议的，可以向ZDHY提出投诉。

8.2 ZDHY对申诉人（投诉人）、申诉（投诉）事项的信息应予以保密，承诺申诉（投诉）的提交、调查和决定不造成针对申诉人/投诉人的歧视。

8.3 ZDHY将及时、公正、有效地处理申诉（投诉），采取必要的措施。与申诉（投诉）事项有直接或间接利害关系的工作人员，应回避该事项的调查处理工作。对申诉（投诉）的处理决定由与申诉（投诉）事项无关的人员做出。ZDHY应及时将处理结果告知申诉人（投诉人）。

9 信息公开

9.1 ZDHY至少在审核实施前3天，将审核计划上报国家认监委（CNCA）相关网站，并应在上报认证证书信息的同时，上报管理体系审核结果信息。

9.2 ZDHY颁发认证证书后，按照国家认监委（CNCA）规定的时限和要求，上报认证结果相关信息，并将认证证书的状态信息在ZDHY网站（www.zdhy.net）公开，供公众查询。

9.3 ZDHY在网站（www.zdhy.net）公开暂停、撤销、注销认证证书的信息。ZDHY暂停认证证书时，将明确暂停的起始日期和暂停期限。ZDHY将在暂停、撤销、注销认证证书之日起

2个工作日内，按规定程序和要求报国家认监委（CNCA）。

10 认证记录

10.1 ZDHY建立认证活动过程记录并妥善保存，归档留存时间为当前认证周期加上一个完整的认证周期。

10.2 认证记录应真实、准确、完整,以证实认证活动得到有效实施。认证记录包括但不限于

（1）认证申请书；

（2）认证申请评审记录；

（3）认证合同；

（4）审核策划及审核计划；

（5）首、末次会议签到表；

（6）现场审核记录；

（7）不符合项报告及验证记录；

（8）审核报告；

（9）认证决定记录。

11 认证收费

11.1 ISMS认证收费项目包括：

（1）申请费：初次认证、再认证、增加认证领域、变更认证范围等的申请费用；

（2）审核费：初次认证审核、监督审核、再认证审核、特殊审核、专项审核等审核活动所发生的费用；

（3）认证决定与注册费（含证书费）：初次认证、再认证、认证变更等认证决定与注册费；

（4）其他费用：如年金、认证标志使用费、换证费、补证费、证书副本费、不符合验证等审核活动所需费用等。

11.2 ISMS 认证项目的基本收费标准如下表所示：

序号	收费项目	收费标准/元
1	申请费	1000
2	审核费	5000×人日数
3	认证决定与注册费（含证书费）	2000
4	年金（含认证标志使用费）	2000
5	换证费/补证费	200
6	副本费	200

序号	收费项目	收费标准/元
7	其他费用	不符合验证等审核活动所需费用

认证项目的最终收费以认证合同约定为准。

12 信息通报

获证组织应及时将可能影响其ISMS持续满足认证要求的有关事宜通知ZDHY，包括但不限于以下信息：

（1）获证组织的法律地位、生产经营状况、组织状态或所有权的变更；

（2）获证组织所取得的行政许可资质证书、强制性产品认证证书或其他资质证书的变更，或到期后未能正常换证的情况；

（3）获证组织的组织机构和管理层重要人员的变更信息；

（4）获证组织的联系地址、生产经营场所的变更信息；

（5）获证组织ISMS及其覆盖范围、过程的重大变更信息；

（6）获证组织的客户及相关方有关ISMS运行的重大投诉信息；

（7）获证组织发生的严重违法失信行为或事件，或发生网络安全事件，已经或可能损害国家安全、社会秩序、公共利益或获证组织及其相关方的合法权益，反映其ISMS的运行存在重大缺陷的信息；

（8）获证组织在认证证书有效期内，受到行政监管部门的处罚，被责令停业整顿，或被列入国家企业信用信息公示系统发布的严重违法失信名单的情况；

（9）获证组织存在影响ISMS有效运行的严重的不符合；

（10）获证组织其他方面的信息（包括因法律法规、标准或其他规范性要求的变更，出现影响ISMS运行的其他重要情况等）。

13 认证数据安全

ZDHY 严格落实《中华人民共和国数据安全法》和《中华人民共和国网络安全法》等法律法规要求，在中华人民共和国境内开展认证活动中收集和产生的重要信息和数据应当在境内存储，确保信息和数据处于有效保护和合法利用的状态未经安全评估和网信等相关部门批准，不向境外传输提供、公开存储于中华人民共和国境内的数据。法律行政法规另有规定的，依照其规定。

14 附则

本认证方案由北京中大华远认证中心有限公司（ZDHY）负责解释。

附录 A

信息安全管理体系认证业务范围分类

信息安全管理体系认证业务范围分类表见表A。

表A　信息安全管理体系认证业务范围分类表

大类	中类	风险级别	描述	备注
01	政务			
	01.01	一级	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	一级	税务机关	
	01.03	一级	海关	
	01.04	二级	其他	例如政党，政协，社会团体等
02	公共			
	02.01	一级	通信、广播电视	
	02.02	一级	新闻出版	包括互联网内容的提供
	02.03	二级	科研	涉及特别重大项目的应提升为一级
	02.04	二级	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	一级	医疗服务	
	02.06	三级	教育	
	02.07	二级	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	一级	金融	例如银行、证券、期货、保险、资产管理等
	03.02	一级	电子商务	以在线交易为主要特点，含网络游戏
	03.03	一级	物流	包括邮政
	03.04	三级	咨询中介	例如法律、会计、审计、公证等
	03.05	二级	旅游、宾馆、饭店	
	03.06	三级	其他	

大类	中类	风险级别	描述	备注
04	产品的生产			产品包括软件、硬件、流程性材料和服务
	04.01	一级	电力	包括发电和输、变、配电等
	04.02	一级	铁路	
	04.03	一级	民航	
	04.04	一级	化工	
	04.05	一级	航空航天	
	04.06	一级	水利	
	04.07	二级	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	二级	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	二级	冶金	
	04.10	二级	采矿	含石油、天然气开采
	04.11	二级	食品、药品、烟草	
	04.12	三级	农、林、牧、副、渔业	
	04.13	三级	其他	

注：认证组织可登录 ZDHY 网站（www.zdhy.net）查看 ZDHY 认可证书附件，具体开展的受认可的认证业务范围可详询 ZDHY 市场服务部 010-87983161/87983114。

附录 B

信息安全管理体系认证审核时间要求

信息安全管理体系认证审核时间计算表见表B。

表B 信息安全管理体系认证审核时间计算表

在组织控制下工作的人员的数量	ISMS初次审核审核时间（第一阶段+第二阶段）（人日）	在组织控制下工作的人员的数量	ISMS初次审核审核时间（第一阶段+第二阶段）（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	/	/

注：

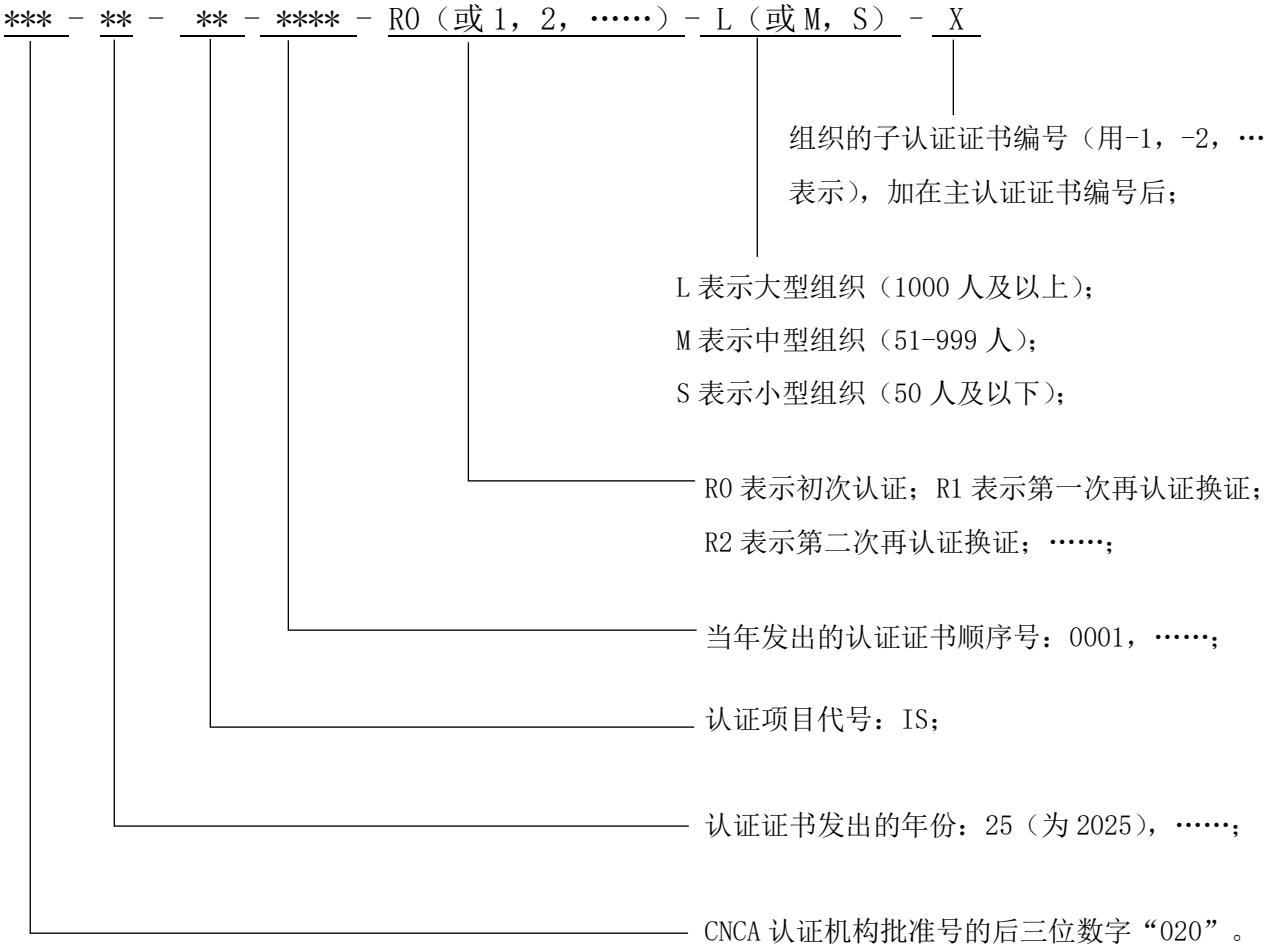
1、往返于多审核场所之间所花费的时间不计入管理体系的认证审核时间；

2、未被指派为审核人员的审核组成员（即技术专家、翻译人员、观察员）和实习审核员所花费的时间不计入管理体系认证审核时间。

附录 C

信息安全管理体系认证证书编号规则

C.1 信息安全管理体系认证证书编号格式如下：



C.2 同一个组织的认证范围覆盖多个场所并需要颁发子认证证书时，在子认证证书编号后加上“-”和序号，如-1（-2，-3，……）

C.3 有效期内换发认证证书，认证证书编号中的机构批准号的后三位数字、年份、顺序号和认证的有效期保持不变，同时注明换证日期。

C.4 再认证完成后换发认证证书，按 C.1 规定重新赋予认证证书编号，第一次再认证为“R1”，第二次再认证为“R2”，依此类推。

C.5 撤销认证证书后，原认证证书编号废止，不再做它用。