信息安全管理体系认证方案

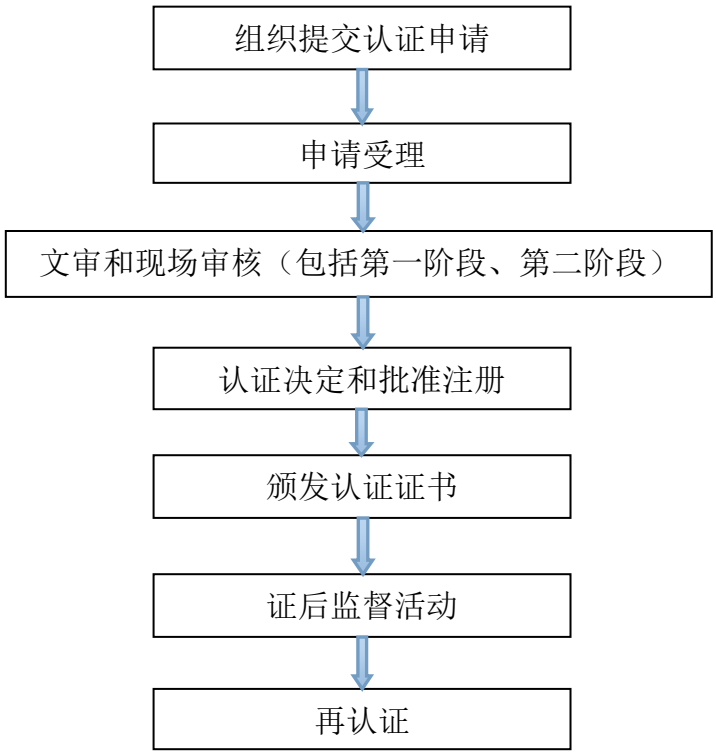
1 适用范围

本认证方案适用于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，其规定了 ISMS 认证的通用要求、特定规则与程序，必要时，在认证合同中补充相关的技术要求。

2 认证模式

ZDHY 首先对认证受审核组织的 ISMS 进行初次审核，经过评定，确认是否批准认证注册；认证注册后，在认证周期内对获证组织的管理体系进行监督和再认证，确认是否持续满足认证要求。

3 认证基本流程：



4 认证依据标准

ISMS 认证依据标准为：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》；

5 认证申请

5.1 申请认证组织的基本条件包括：

（1）申请认证的组织应具有明确的法律地位，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）在国家地方或行业有要求时，申请组织应具有规定的资质，其申请认证范围应在法律地位文件和资质规定的范围内；

（3）申请组织应按现行有效的认证依据标准建立和实施了文件化的 ISMS，一般情况下体系需有效运行 3 个月以上，且至少已实施一次完整内审和管理评审（适用于初次认证）；

（4）申请组织近一年内，未受到政府主管部门行政处罚。如果曾获得过 ISMS 认证证书，其证书在有效期内未被认证机构撤销；

（5）适用时，申请的认证范围所覆盖的产品和服务涉及法律法规要求的行政许可或强制性认证时，应具有相应的证书并保持有效；

（6）申请组织承诺遵守国家的法律、法规其他要求，承诺始终遵守认证的有关规定，承诺按合同约定和法律规定承担与认证有关的相关法律责任；

（7）申请组织承诺获得 ZDHY 认证证书后，持续有效运行 ISMS，按认证合同约定支付有关费用，按规定接受 ZDHY 和认证监管部门的监督/检查，按 ZDHY 规定使用认证证书、标志和审核报告，并将组织发生的可能影响 ISMS 持续满足认证标准要求的能力的事宜向 ZDHY 报告。

5.2 申请 ISMS 认证的组织需遵守的特定要求

（1）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/监管部门对信息安全管理体系认证的管理要求，中心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。

（2）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。

5.3 为了确保认证的有效性，规避认证风险，中心暂不接受由其他认证机构颁发的现行有效的信息安全管理体系认证证书转为本中心的认证证书，所有认证申请均按初次认证程序要求执行。

5.4 ZDHY 制定公开文件公开认证过程的适当信息，拟申请认证的组织可以通过 ZDHY 网站（www.zdhy.net）或联系电话，下载或索取

ZDHY 的公开文件，了解 ISMS 认证的基本要求及相关信息，符合认证基本要求的组织即可向 ZDHY 提交认证申请。

5.5 申请组织的授权代表应按要求向 ZDHY 提供《认证申请书》及其相关资料，包括以下必要的信息：

（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）申请组织的相关详细情况，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、人力资源和技术资源、职能、关系以及班次；

（3）申请组织任何相关的法律义务，包括：

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（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）；

② 取得相关法规规定的行政许可文件（适用时）；

③ 从事的业务活动符合我国相关法律法规、标准和有关规范的要求；

（4）已按照适用的认证依据标准要求，建立和实施了文件化的 ISMS，且体系有效运行时间超过 3 个月；

（5）已策划并实施完成内部审核和管理评审；

（6）申请组织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）是否接受过与拟认证的管理体系有关的咨询，如果接受过，由谁提供咨询；

（8）识别并向中心告知其 ISMS 范围内的哪些信息资产不允许中心接触，或者中心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、需要通过信息安全管理体系应对的要求和组织自身的要求，中心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；

（9）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），以便中心确定 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。

6 申请受理

6.1 申请评审

6.1.1 ZDHY 确认收到的认证申请资料是否齐全，并对认证申请及相关文件化信息进行评审，必要时，要求申请组织补充信息。

6.1.2 在申请评审后，ZDHY 决定是否受理认证申请。如果拒绝认证申请会清楚告知申请组织被拒绝的原因。

6.2 签订认证合同

ZDHY 决定受理认证申请后，在实施认证审核前，ZDHY 与申请组织签订具有法律效力的书面认证合同。

7 初次认证审核

初次 ISMS 认证审核分为两个阶段实施，即第一阶段和第二阶段审核。

7.1 第一阶段审核

7.1.1 第一阶段审核的目的是通过了解受审核组织的 ISMS 及其现场运作，确定受审核组织为第二阶段审核的准备情况，并为策划第二阶段审核提供关注重点。第一阶段审核在申请组织的现场进行，并至少包含以下审核内容：

（1）获取受审核组织的 ISMS 设计的文件，包括认证依据标准所要求的文件，充分了解在组织环境下所进行的 ISMS 设计、风险评估和处置（包括所确定的控制）、适用性声明的选择及删减的合理性、信息安全方针和目标，初步评价其与依据标准的符合性；

注：当受审核组织由于信息安全的原因在申请评审阶段不能提供给 ZDHY 足够的信息时，ZDHY 将通过第一阶段审核在现场补充对上述信息的确认，并完成申请评审任务。这种情况下，ZDHY 会增加第一阶段现场审核时间。

（2）评价 ISMS 覆盖的运作场所和现场的具体情况，并与受审核组织的相关人员进行讨论，确定第二阶段审核的准备情况；

（3）审核受审核组织理解和实施认证依据标准要求的情况，特别

是对 ISMS 的关键绩效、过程、目标和运作的识别情况；

（4）收集关于受审核组织的 ISMS 范围的必要信息，包括过程、场所及控制程度、适用的法律法规要求和遵守情况；

（5）审核第二阶段审核所需资源的配置情况，并与受审核组织商定第二阶段审核的详细安排；

（6）结合认证依据标准或其他规范性文件充分了解受审核组织的 ISMS 和现场运作，以便为策划第二阶段提供关注点；

（7）评价受审核组织的 ISMS 的运行情况，是否有足够的证据证明其审核 ISMS 已有效运行超过 3 个月，并实施了内部审核与管理评审，以便证明已为第二阶段做好准备。

7.1.2 ZDHY 应将第一阶段目的是否达到、第二阶段是否准备就绪的书面结果告知受审核组织，包括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。如果第一阶段审核提出影响实施第二阶段审核的问题，这些问题应在第二阶段审核前得到解决。第二阶段可以要求对更进一步的信息和记录做详细检查。

7.1.3 ZDHY 在确定第一阶段和第二阶段的间隔时间时，需考虑受审核组织解决第一阶段识别的任何需关注问题所需的时间。

7.1.4 第一阶段的结果可能导致推迟或取消第二阶段。如果受审核组织发生任何将影响 ISMS 的重要变更，ZDHY 考虑是否有必要重复整个或部分第一阶段。

7.2 第二阶段审核

第二阶段审核的目的是评价受审核组织 ISMS 的实施情况符合性和有效性，确认受审核组织遵守自身的方针、策略和规程。第二阶段审核在受审核组织现场进行，并至少覆盖以下审核内容：

（1）受审核组织 ISMS 实施与认证依据标准要求的符合情况及其证据；

（2）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；

（3）受审核组织 ISMS 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；

（4）受审核组织对 ISMS 覆盖的过程和活动的管理及控制情况；

（5）受审核组织的内部审核和管理评审的有效性；

（6）针对受审核组织的方针的管理职责；

（7）重点关注的审核内容：

① 最高管理者的领导力和对信息安全方针与信息安全目标的承诺；

② 认证依据标准中的文件要求；

③ 评估与信息安全有关的风险，以及评估可产生一致的、有效的、在重复评估时可比较的结果；

④ 基于风险评估和风险处置过程，确定控制目标和控制情况；

⑤ 信息安全绩效和 ISMS 有效性，以及根据信息安全目标对其进行监视、测量和评审；

⑥适用性声明中所必需的控制以及条款删减的理由、风险评估与风险处置过程的结果、信息安全方针与目标，它们相互之间的一致性；

⑦ 控制的实施，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和控制的监视、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；

⑧ 方案、过程、规程、记录、内部审核和对 ISMS 有效性的评审，以确保其可被追溯至管理决定和信息安全方针与目标；

⑨ 受审核组织对信息安全相关风险的评估与ISMS范围内的ISMS运行是相关的和充分的；

⑩ 受审核组织识别、检查和评价信息安全相关风险的规程及其实施结果是否与受审核组织的方针、目标和指标相一致；

⑪ 确定用于风险评估的规程是否健全并得到正确实施。

7.3 初次认证的审核结论

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分析，以评审审核发现并就审核结论达成一致。

8 现场审核实施

8.1 由代表 ZDHY 的审核组实施现场审核，要求受审核组织证实对信息安全相关风险的评估与 ISMS 范围内的 ISMS 运行是相关的和充分的，确定受审核组织识别、检查和评价信息安全相关风险的规程及其实施结果是否与方针、目标和指标相一致，还应确定用于风险评估的规程是否健全并得到正确实施。

8.2 审核组在现场审核前，通过审查受审核组织的 ISMS 的文件、

与受审核组织沟通，了解受审核组织的有关信息，制定审核计划，确认审核安排，说明首末次会议议程。

8.3 审核组按照审核计划中审核内容和日程安排实施审核，在审核现场与受审核组织的管理层召开正式的首次会议，告知双方的职责和义务，介绍审核安排并解释审核活动和方式。

8.4 审核组在审核现场活动中，通过与过程和活动的岗位人员面谈、查阅文件化信息、观察产品和服务形成过程、活动等适当方法，抽样收集并验证有关的信息，形成审核证据，确定审核发现。在末次会议前，审核组对照审核目的和审核准则，审查审核发现和审核中获得的适用信息，就审核结论和必要的后续跟踪活动达成一致。

8.5 审核组及时与受审核方沟通，沟通的内容包括：

（1）通报审核进程；

（2）确认审核发现中的不符合事实；

（3）解决与审核证据或审核发现分歧意见；

（4）当审核发现表明不能达到审核目的时，应说明理由，商定后续措施；

（5）在末次会议前，审核组长与受审核组织管理层沟通现场审核的信息，确认审核结论，并商定后续措施的安排。

8.6 在现场审核结束前，审核组与受审核组织的管理层召开正式的末次会议，提出审核发现（包括不符合）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回应的时间表达成一致。

8.7 审核组如果需要改变审核目的和范围或终止审核时，应经ZDHY 评审和批准后实施。对终止审核的项目，审核组应将已开展的工作情况形成报告，ZDHY 将此报告及终止审核的原因提交受审核组织。

9 审核报告

9.1 审核组长负责编制审核报告，审核报告应准确、简明和清晰地描述审核实施的主要内容，以及提出不符合的纠正和纠正措施有效性验证结果、审核结论（包括关于认证的推荐性意见）。在审核结束后，将审核报告和相关的审核记录、不符合报告及纠正措施证实性文件化信息提交 ZDHY，用以支持 ZDHY 作出认证决定。

9.2 ZDHY 享有对审核报告的所有权。经 ZDHY 批准后，向受审核组织提供审核报告。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。

10 认证决定

10.1 ZDHY 对审核组提交的审核报告、不符合的纠正和纠正措施及实施证据等信息进行审查，确定认证要求满足程度和认证范围，接受和验证了不符合的纠正和纠正措施。

10.2 如果在第二阶段结束后 6 个月内，不符合的纠正和纠正措施不能得到审核组或 ZDHY 接受和验证，则审核组在推荐认证前要再实施一次第二阶段审核。

10.3 在对审核组提供的信息有效审查的基础上，综合考虑审核组关于认证的推荐性意见和其它来源获得的补充信息，做出认证决定。

10.4 ZDHY 认为申请组织具备充分的证据证实管理评审和 ISMS 内部审核的安排已经实施，并且保持有效，在认证范围内已满足授予认证资格条件，做出同意授予认证的决定。经 ZDHY 主任批准后，向申请组织颁发 ISMS 认证证书和相关文件，并要求获证组织按 ZDHY 要求正确使用认证证书、标志和向 ZDHY 通报相关信息。

10.5 对于不符合认证要求的申请人，ZDHY 以书面的形式告知其不能通过认证的原因。

11 认证证书

ISMS 认证证书有效期一般为 3 年。认证证书内容包含以下信息：

（1）获证组织名称、注册地址和统一社会信用代码（组织机构代码）；

（2）ISMS 覆盖的生产经营或服务的地址和业务范围。若认证的 ISMS 覆盖多场所，表述覆盖的相关场所的名称和地址；

（3）ISMS 符合认证依据标准的表述；

（4）ISMS 适用性声明的版本；

注：如果适用性声明的变更没有改变认证范围中控制措施的覆盖范围，则不要求更新认证证书。

（5）认证用标准和（或）其他规范性文件所要求的任何其他信息；

（6）在颁发更换的认证证书时，在认证证书上标明换证日期；

（7）证书编号；

（8）ZDHY 名称和标志、地址；

（9）证书签发人、发证日期（即生效日期）及有效期的截止日期；

（10）适用时，相关的认可标识及认可注册号；

（11）证书查询方式。

12 证后监督

12.1 监督活动的方式

监督的目的是验证已被认证的 ISMS 得到持续实施、考虑获证组织运作变化所引起的 ISMS 变化的影响，并确认与认证要求的持续符合。ZDHY 采用现场监督审核和日常监督相结合的方式。

12.2 日常监督活动可包括：

（1）获证组织信息通报制度；

（2）ZDHY 就认证的有关方面询问获证组织；

（3）审查获证客户对其运作的说明（如宣传材料、网页）；

（4）要求获证客户提供文件化信息（纸质或电子介质）；

（5）其他监视获证客户绩效的方法（如关注国家有关部门发布的信息公报、关注获证组织相关方及媒体的信息等）。

12.3 监督审核

12.3.1 监督审核应在获证组织现场进行，每次监督审核的内容至少包括：

（1）ISMS 变更的策划及实施过程、及其引起的适用性声明（SoA）变更和其他任何变更（如资源、组织结构、关键管理人员等）；

（2）控制的实施和有效性；

（3）ISMS 在实现获证组织信息安全方针、目标和 ISMS 预期结果方面的有效性；

（4）内部审核和管理评审；

（5）申诉和投诉的处理，在发现任何不符合或不满足认证要求时，检查获证组织是否对其自身的 ISMS 和规程进行了调查并采取了适当的纠正措施；

（6）为持续改进而策划的活动的进展；

（7）对上次审核中确定的不符合所采取的措施；

（8）对与相关信息安全法律法规的符合性进行定期评价与评审的规程的运行情况；

（9）认证证书和标志的使用和（或）任何其他对认证资格的引用。

12.3.2 为使现场审核活动能够观察到 ISMS 范围内的业务活动情况，现场审核应安排在认证范围覆盖的业务活动正常运行时进行。由于获证

组织业务运作时间（季节性）特点，在每次监督审核时难以覆盖所有业务活动的，在认证证书有效期内的监督审核必须覆盖 ISMS 认证范围内的所有业务活动。

12.3.3 监督审核的频次

在证书有效期内，获证组织须接受监督审核。第一次监督审核的时间为自初次认证决定日期（认证证书的发证日期）起 12 个月内。第二次及以后监督审核时间间隔为自上次监督审核日期起 12 个月；即正常情况，每年须接受一次监督审核。

若发生下述情况则需增加监督频次。必要时，安排提前较短时间通知的审核：

（1）获证组织对 ISMS 进行了重大变更；

（2）有足够信息表明获证组织发生了组织机构、场所、业务活动变更等影响到其认证基础的更改；

（3)获证组织出现相关方提出对 ISMS 运行效果的投诉未回应时；

（4）对被暂停认证资格的获证组织进行追踪；

（5）其他需要考虑的情况。

12.4 ZDHY 根据现场监督审核和日常监督的结果，对获证组织作出保持、暂停、或撤销其认证资格的决定，并以书面形式告知获证组织。

13 再认证

13.1 再认证目的是验证作为一个整体的组织 ISMS 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。

13.2 ISMS 认证证书有效期截止日期前 4 个月，需要延续认证有效期的获证组织必须向 ZDHY 提出再认证申请，ZDHY 按照第 6 条规定要求实施再认证申请评审。

13.3 ZDHY 在前认证证书有效期截止日期前安排再认证审核，再认证审核按照第 7 条规定的初次认证审核程序要求实施。

13.4 当管理体系、获证组织或管理体系的运作环境（如法律的变更）无重大变更时，再认证审核活动可省略第一阶段，否则再认证审核活动需要进行第一阶段。

13.5 根据再认证审核的目的，再认证审核包括针对下列方面的现场审核：

（1）结合内部和外部变更来看的整个 ISMS 的有效性，以及认证范

围的持续相关性和适宜性；

（2）经证实的对保持 ISMS 有效性并改进管理体系，以提高整体绩效的承诺；

（3）ISMS 在实现获证组织信息安全目标和 ISMS 预期结果方面的有效性。

13.6 对于审核组提出的不符合，受审核组织要在规定的时限内实施纠正和纠正措施，并确保在认证证书有效期截止日期前得到审核组和 ZDHY 对实施有效的验证。

13.7 根据再认证审核的结果，以及认证周期内 ISMS 评价结果和认证相关方投诉的信息，ZDHY 分别做出以下的认证决定：

13.7.1 在认证证书有效期截止日期前，ZDHY 接受和验证了纠正和纠正措施，且认为符合认证注册授予条件，做出同意再认证的决定，换发认证证书。新认证证书发证日期为再认证决定日期，有效期 3 年。如果申请再认证组织提出要求，新认证证书的有效期截止日期与前认证证书的有效期截止日期相距 3 年。对在 ZDHY 初次认证以来未中断过的再认证证书，可注明 ZDHY 初次认证证书的发证日期。

13.7.2 在认证证书有效期截止日期前未能完成再认证审核或不能验证对不符合实施的纠正和纠正措施，ZDHY 做出不能延续认证的决定，同时告知获证组织并解释后果。

13.7.3 在认证证书有效期截止日期之后 6 个月内，完成未尽的再认证活动，符合认证注册授予条件，ZDHY 做出同意恢复再认证的决定。重新颁发认证证书的发证日期为恢复再认证决定日期，新认证证书的有效期截止日期与前认证证书的有效期截止日期相距 3 年，即重新颁发的认证证书有效期不足 3 年。

13.7.4 在认证证书有效期截止日期之后 6 个月内，不能完成再认证审核并接受和验证了纠正和纠正措施，ZDHY 做出拒绝再认证的决定。如果原获证组织考虑获得认证资格，需要按照初次认证的程序再次提出认证申请。

14 扩大或缩小认证范围

14.1 扩大认证范围

14.1.1 在认证证书有效期内，需要扩大认证范围的获证组织应向 ZDHY 正式提交扩大认证范围的申请和相关文件化信息。

14.1.2 ZDHY 针对获证组织提出扩大认证范围的申请和相关文件化信息进行评审，确定予以扩大的决定所需的审核活动，该审核可与监督审核同时进行。

14.1.3 经 ZDHY 实施相关审核和审定，确定获证组织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，换发认证证书。认证证书的证书号和有效期截止日期保持不变，并注明原证书发证日期。

14.2 缩小认证范围

14.2.1 在认证证书有效期内，需要缩小认证范围的获证组织应向 ZDHY 正式提交缩小认证范围的申请，或由 ZDHY 审核组通过审核提出缩小获证组织认证范围的建议，并提供理由和证据。ZDHY 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。需要时，获证组织与 ZDHY 补充签订认证合同/协议。

14.2.2 经 ZDHY 审定，决定获证组织缩小认证范围后不会对仍保持的认证范围产生影响，满足缩小认证范围批准认证资格的条件，同意批准缩小认证范围，换发认证证书或附件。认证证书的证书号和有效期截止日期保持不变，并注明原证书发证日期。

14.2.3 获证组织在收到换发的认证证书时必须交回原认证证书。并按照 ZDHY 的要求，正确使用缩小/变更范围后的认证证书，同时按缩小/变更的认证范围修改其广告及相关宣传材料。

15 变更认证证书

15.1 当认证证书所覆盖的获证组织名称、注册地址、业务范围、场所地址、认证要求（包括认证标准换版）等内容发生变化，获证组织应按照 ZDHY 的相关要求，提出认证证书变更申请。

15.2 对获证组织名称、地址信息发生变化的认证证书变更申请，经申请评审确认，必要时，由审核组现场审核并确认。当证实组织名称、地址信息变更符合认证授予条件，ZDHY 做出同意变更认证证书的决定。

15.3 对获证组织认证证书所覆盖的业务范围、场所地址、认证要求（包括认证标准换版）发生变更的认证证书变更申请，通过申请评审安排审核组进行现场审核并确认，变更的业务范围、场所地址、认证要求（包括认证标准换版）符合认证授予条件，ZDHY 做出同意变更认证

证书的决定。

15.4 通过监督审核和再认证审核，发现认证证书所覆盖的业务范围、场所地址、认证要求（包括认证标准换版）发生变化，由审核组在现场审核中确认并报 ZDHY 进行评审和审查，变更的业务范围、场所地址、认证要求（包括认证标准换版）能够符合认证授予条件，ZDHY 做出同意变更认证证书的决定。

15.5 在认证证书有效期内，因证书所覆盖的获证组织名称、业务范围、场所地址、认证要求（包括认证标准换版）等内容变更而换发认证证书，其证书号和认证有效期截止日期保持不变，并注明原证书发证日期。

15.6 当认证证书所覆盖的获证组织名称、注册地址、业务范围、场所地址、认证要求（包括认证标准换版）等内容发生涉及扩大或缩小认证范围，ZDHY 按照第 14 条要求执行。

16 暂停、恢复认证证书

16.1 暂停认证证书

16.1.1 在认证证书有效期内，通过证后监督、审核、审定、体系评价结果和相关方投诉信息，获证组织发生不能保持认证的情况，ZDHY 提出对获证组织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。必要时，ZDHY 与获证组织沟通，核实证据。

16.1.2 经 ZDHY 审定，确认获证组织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，满足暂停认证资格的条件，同意批准暂停全部或部分认证范围的认证资格，暂停期限为六个月。并向获证组织颁发《暂停使用认证证书的通知》并在 ZDHY 网站上公布。

16.1.3 被暂停认证资格的获证组织要按照 ZDHY 的要求，从暂停决定之日起停止使用认证证书和认证标志，以及任何其他对认证资格的引用。

16.2 恢复认证证书

16.2.1 当暂停的获证组织在要求的时间内解决了造成暂停的问题，经确认符合中心相关规定，报中心主任批准后恢复认证证书使用。

16.2.2 在确定的认证资格暂停限期结束前，经 ZDHY 确认获证组织在暂停认证资格的认证范围内已恢复符合相关的认证要求，做出同意

恢复认证资格的审定结论，颁发《恢复使用认证证书通知》并在 ZDHY 的网站上公告。

16.2.3 恢复认证资格的获证组织要按照 ZDHY 的要求，从恢复决定之日起恢复使用认证证书和认证标志，以及任何其他对认证资格的引用。

17 撤销认证证书

17.1 在认证证书有效期内，通过证后监督、审核和相关方投诉信息，获证组织已不再满足认证的要求，ZDHY 提出对获证组织撤销认证资格的建议，并提供理由和证据。必要时，ZDHY 与获证组织沟通，核实证据。

17.2 经 ZDHY 审定，确定获证组织满足撤销认证的条件，同意批准撤销认证资格。并向获证组织发放《撤销使用认证证书的通知》并在 ZDHY 网站上公布。

17.3 被撤销认证资格的获证组织要按照 ZDHY 的要求，交回认证证书，并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。

18 认证公告

ZDHY 对授予认证的组织名称、认证范围及地理位置，以及保持、更新、暂停、恢复或撤销认证的信息，在 ZDHY 官方网站（www.zdhy.net）上公布。

认证证书相关信息还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。

19 其他要求

19.1 实施本规则的费用按照 ZDHY 公开文件《ISMS/ITSMS 认证申请指南及认证收费标准》执行。

19.2 在本方案实施中，相关方的申诉、投诉和争议的处理按照 ZDHY 公开文件《中心对申诉、投诉和争议处理办法》执行。

19.3 在本规则实施中，授予、拒绝、保持、更新、暂停、恢复或撤销认证或者扩大或缩小认证范围的条件按照 ZDHY 公开文件《认证中心对授予、保持、扩大、更新、缩小、暂停/恢复、撤销及注销认证条件的规定》执行。

19.4 获证组织按照 ZDHY 公开文件《认证/认可标识（牌）使用和

认证证书管理规定》的要求正确使用认证证书、认证标识和认可标识。

19.5 按照 ZDHY 公开文件《获证组织信息通报制度》的要求，获证组织及时将可能影响管理体系持续满足认证标准要求的能力的事宜通知 ZDHY。

20 附则

本规则由北京中大华远认证中心有限公司（ZDHY）负责解释。