基于ISO/IEC 27040的数据存储安全管理体系认证规则

1.适用范围

1.1　本规则用于规范湖北光谷标准创新科技有限公司（以下简称“标创公司”）对申请认证和获证的各类组织按照ISO/IEC 27040:2015《信息技术-安全技术-存储安全》开展的基于ISO/IEC 27040的数据存储安全管理体系认证活动。

1.2　本规则旨依据认证认可相关法律法规及认可规范，对基于ISO/IEC 27040 的数据存储安全管理体系（以下简称“数据存储安全管理体系”）认证规则实施过程作出具体规定，强化标创公司对认证过程的管理和责任，保证数据存储安全管理体系认证规则认证规则活动的规范有效。

1.3　本规则是对标创公司从事数据存储安全管理体系认证规则的认证活动中的基本要求，认证双方在该项认证活动应当遵守本规则。

2.认证依据

2.1　ISO/IEC 27040:2015《信息技术-安全技术-存储安全》；

2.2　CNAS-CC01:2015《管理体系认证机构要求》；

2.3　IAF强制性文件

2.4　GB/T19011-2021/ISO 19011:2018《管理体系审核指南》

3.对认证机构的基本要求

3.1 本机构获得国家认监委批准、取得从事质量管理体系认证、环境管理体系认证和职业健康安全管理体信息安全管理体系、信息技术服务管理体系认证的资质。

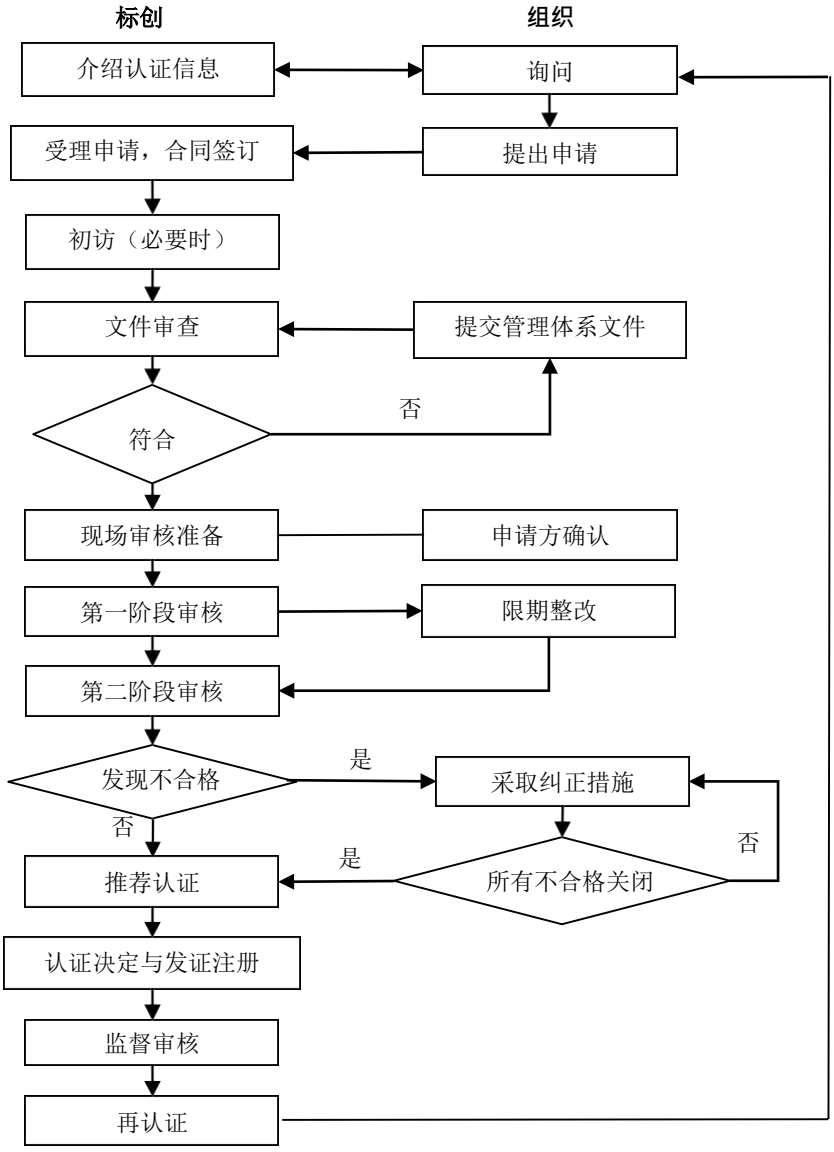
3.2 认证能力、内部管理和工作体系符合GB/T 27021/ISO/IEC 17021-1《合格评定 管理体系审核要求》，以使从事的基于数据存储安全管理体系认证规则认证活动符合相关法律法规及技术标准的规定。

3.3 建立内部制约、监督和责任机制，实现培训（包括相关增值服务）、审核和作出认证决定等工作环节的相互分开，以确保认证审核的公正性。

3.4 适时申请通过认可机构的认可，证明其从事的基于数据存储安全管理体系认证规则认证能力符合要求。

3.5 不得将申请认证的组织（以下简称申请组织）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。

3.6 认证流程



4.对认证人员的基本要求

4.1 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质量管理体系、环境管理体系、职业健康安全管理体系、信息安全管理体系、信息技术服务管理体系等任一一个

管理体系审核员注册资格。

4.2 认证审核员完成相应的基于数据存储安全管理体系认证 规则培训，并考核合格。

4.3 认证人员应当遵守与从业相关的法律法规，具有从事认证工作的基本职业操守，对认证活动及作出的认证审核报告和认证结论的真实性承担相应的法律责任。

4.4 申请方/受审核方的义务

(1) 按标创公司要求提交申请文件及其附件；

(2) 为标创公司提供保证审核工作顺利进行必要的食、宿、行及办公条件；

(3) 为标创公司审核组进入审核区域、调阅文件记录、安排被访问人员等提供必要的条件；适用时，为接纳到场的观察员（如认可机构评审员）提供条件。

(4) 保留顾客和/或相关方就获证组织的活动、产品或服务所提出的所有投诉记录，信息沟通记录及相应纠正措施记录，并在标创公司要求时提供。重要投诉应及时通报标创公司。

(5) 按规定及时交纳认证费用。

5. 认证程序

5.1 认证申请

5.1.1 本机构应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，以及分包境外机构业务的情况；

（2）开展数据存储安全管理体系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）认证证书有效、暂停、注销或者撤销的状态

（8）对认证过程和结果的申诉、投诉规定；

（9）认证标准换版的规定（必要时）；

（10）本认证实施规则；

（11）其他需要公开的信息。

5.1.2 申请数据存储安全管理体系认证的企业应满足以下条件：

- 取得法人资格（或其组成部分）；
- 从业条件中，有行政许可要求的，应取得相应资格并在有效期内；
- 已按认证标准建立数据存储安全管理体系，体系有效运行三个月以上，至少完成一次内部审核，并进行了管理评审；
- 未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未被列入“严重违法失信企业名单”；
- 一年内未发生行政监管部门责令停产整顿的重大事故；
- 一年内未发生国家监督抽查（以下简称“国抽”）不合格，或发生国抽不合格但已按相关规定整改合格；
- 其他应具备的条件。
- 产品及服务符合国家相关法律法规和标准要求；
- 已着手建立文件化的管理体系；
- 本年度无重大与拟申请认证领域相关的责任事故；
- 符合上述条件的标创公司所撤销的组织，可随时提出认证申请，但组织应进行了彻底整改，确保导致辙销认证证书的情形已消除，否则不应受理其认证申请；被其他认证机构撤销资产证书不满 1 年的组织，原则上不应受理其认证申请。

5.1.3 申请方应当向标创公司提交以下资料：

（1）认证申请书，包括认证委托人的名称、地址、认证标准、申请的认证范围、认证范围内组织人员数量及影响体系有效性的外包过程；

（2）法律地位的证明性文件，当数据存储安全管理体系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性文件；

（3）申请认证范围所涉及的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；

（4）组织机构及职责（可随体系文件）；

（5）工艺流程/服务流程及生产和（或）服务的班次及轮班情况（必要时）；

（6）数据存储安全管理体系运行满足三个月的证据；

（7）一年内所发生的数据存储安全管理体系相关的行政处罚、国抽不合格，一年内所发生的其他相关抽查不合格的情况以及整改情况；

（8）企业数据存储安全管理体系成文信息 (适用时)。

（9）其他需要提供的文件。

5.1.4 申报企业要诚实守信，如实申报。对提供虚假材料的企业，在 3 年内不再受理相关申请。

5.1.5 申请方应填写《管理体系认证申请书》，认证机构在收到申请之后，做出受理与否的书面答复。

5.1.6 接受申请后，双方协商，认证机构与申请方签订《管理体系认证合同》。

5.1.7 若评审结论为不予受理，认证机构应当以书面形式通知申请方。

5.1.8 申请方对不予受理有异议的，可以向认证机构申诉。对认证机构处理结果仍有异议的，可以向国家认监委投诉。

5.2 申请评审

5.2.1按照本机构申请评审程序，对认证委托人提交的申请文件和资料实施申请评审，根据申请认证的活动范围及场所、员工人数、完成审核所需时间和其他影响认证活动的因素，综合确定是否有能力受理认证申请并保存相应评审记录。

对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”的申请组织，认证机构不应受理其认证申请。

5.2.2 满足以下条件的，本机构可以受理认证申请：

（1）认证委托人已具备受理条件（见5.1.2）；

（2）本机构具备实施认证的能力；

（3）双方就认证事宜达成一致。

5.2.3 对于新的认证委托人，本机构按照初次认证开展认证活动，无论其是否持有其他机构颁发的数据存储安全管理体系有效证书。

5.2.4 本机构应将申请评审的结果告知认证委托人，要求补充和完善，或者不受理认证申请。

5.3 认证合同

5.3.1 通过申请评审的，在实施认证审核前，本机构应与认证委托人签订具有法律效力的认证合同，以明确认证委托人和本机构的责任。

5.3.2 本机构的责任至少包括：

（1）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，通过网站或者其他形

式向社会公布获证信息；

（2）对获证组织数据存储安全管理体系运行情况进行有效监督，发现获证组织的数据存储安全管理体系不能持续符合认证要求的，应及时暂停或者撤销其认证证书;

（3）因本机构原因（如机构认证资质被注销或撤销）导致获证组织数据存储安全管理体系证书无法有效保持的，需及时告知获证组织并做出妥善处理。

5.3.3 获证组织的责任至少包括：

（1）遵守认证程序要求，认证过程如实提供相关材料和信息，通过数据存储安全管理体系认证后持续有效运行数据存储安全管理体系；

（2）申请组织对遵守认证认可相关法律法规，配合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的承诺。配合本机构对投诉的调查；

（3）应当在广告、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，不利用数据存储安全管理体系认证证书和相关文字、符号误导公众认为其产品或服务通过认证;

（4）发生如下情况，应及时向本机构通报：发生重大事故、受到监管部门行政处罚、监管部门公布存在安全生产不符合、被媒体曝光存在重大问题、数据存储安全管理体系不能正常运行或发生重大变更，以及其他应通报的情况、客户及相关方有重大投诉，相关情况发生变更，包括：法律地位、生产经营状况、组织状态或所有权变更；取得的行政许可资格、强制性认证或其他资质证书变更；法定代表人、最高管理者变更；生产经营或服务的工作场所变更；数据存储安全管理体系覆盖的活动范围变更；数据存储安全管理体系和重要过程的重大变更，出现影响数据存储安全管理体系运行的其他重要情况等;

（5）承担选择本机构的风险，如：因本机构资质被撤销而带来的认证证书无法使用的风险；

（6）按合同约定及时向本机构缴纳认证费用。

5.4 审核方案和审核策划

5.4.1 审核方案

5.4.1.1 本机构应针对每一认证委托人建立认证周期内的审核方案，以清晰地识别所需的审核

活动。

5.4.1.2 初次认证的审核方案应包括两阶段初次审核、获证后的监督审核和认证到期前进行的再认证审核。

注：一个认证周期通常为3年，从初次认证（或再认证）决定算起，至认证的有效期截止。

5.4.1.3 初次认证审核和再认证审核是对认证委托人完整体系的审核，应覆盖ISO/IEC 27040所有要求，以及认证范围内的典型产品和服务。认证证书有效期内的监督审核应覆盖ISO/IEC 27040所有要求。

5.4.1.4 初次认证及再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。

5.4.1.5 如果机构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。机构应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

5.4.1.6 本机构应考虑认证委托人不同班次完成的过程，以及其所证实的对每个班次的数据存储安全管理体系控制水平来策划对不同班次实施的审核程度，以确保审核的有效性：

（1）每次审核应至少对其中的一个班次的生产或服务的活动现场进行审核；

（2）对于未审核的班次，应记录不对其审核的理由。

5.4.2 审核时间

5.4.2.1 审核时间包括在认证委托人现场的审核时间以及在现场审核以外的实施策划、文件审核和编写审核报告等活动的时间。审核时间以人天计，1人天为8小时。如果每天的实际工作时间不足8小时，则应延长审核天数以满足人天要求。基于数据存储安全管理体系的审核时间与信息安全管理体系的审核时间相同。若申请方已获得GB/T 22080(ISO/IEC 27001,IDT)有效认证证书，并且范围覆盖了基于数据存储安全管理体系申请范围，则基于数据存储安全管理体系的审核时间数按照信息安全管理体系的审核时间的0.5 倍+1天进行计算（向上取整至0.5人天），当GB/T22080(ISO/IEC 27001,IDT)证书由北京埃尔维质量认证中心颁发时，则基于数据存储安全管理体系的审核时间数按照信息安全管理体系的审核时间的0.5 倍进行计算（向上取整至0.5人天）。

5.4.2.2 本机构应以附录A所规定的审核时间为基础，考虑认证委托人有效人数等因素，建立文件化的不同类型审核的审核时间（包括现场审核时间）的确定方法。

5.4.2.3 每次审核的审核时间的确定过程应形成记录，尤其是减少审核时间的理由，减少的时间不得超过附录A所规定的审核时间的30%，现场审核时间不得少于所确定的审核时间的80%。

5.4.2.4 本机构应建立结合审核时间的确定方法，数据存储安全管理体系和其他管理体系实施结合审核时，结合审核的总审核时间不得少于多个单独体系所需审核时间之和的80%。

5.4.3 多场所抽样方案

5.4.3.1 本机构应建立并实施多场所组织认证抽样的规则并遵照执行，策划并保留多场所组织的抽样及确定审核时间的记录。

5.4.3.2 多场所抽样应基于与认证委托人活动或过程性质相关的数据存储安全管理体系风险的评价，如果多个场所未涵盖相同的活动、过程及数据存储安全管理体系风险类型，则不应抽样，应当逐一到各场所进行审核。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。

5.4.3.3分场所审核人日的计算方法参见5.4.2，且现场审核时间不得少于依据附录A所确定的现场审核时间的50%。

5.4.4 组建审核组

5.4.4.1 本机构应根据实现审核目的所需的能力和公正性要求组建审核组，必要时可以选择技术专家参加审核组。审核组中的审核员承担审核任务和责任,每个审核组应包括：

（1）审核组长，本机构应建立审核组长的选择、培训以及任用的管理制度，审核组长应

当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/T19011《管理体系审核指南》标准中对审核组长的通用要求;

（2）数据存储安全管理体系和其他管理体系实施结合审核的，审核组应包括其他管理体系的人员，确保人员的能力覆盖实施结合审核的全部管理体系;

5.4.4.2 审核组成员不得与认证委托人存在利益关系。

5.4.5 远程审核方法

5.4.5.1 数据存储安全管理体系认证审核应在认证委托人的现场实施，初次认证以及认证周期内的每年度的监督审核和再认证审核活动，应包括访问认证委托人现场的现场审核。

5.4.5.2 因安全因素的考虑，审核组可在认证委托人的现场采用远程审核方法对认证委托人的某个过程的运作情况实施审核。

5.4.5.3 审核中采用远程审核方法的，远程审核时间不得超过现场审核时间的30%，并应在审核计划、审核记录及审核报告中予以注明。

5.4.6 审核计划

5.4.6.1 本机构应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、审核准则、审核范围、现场审核的日期、时间安排和场所、审核组成员及审核任务安排。其中，审核员应注明审核员注册号，如聘请了技术专家，应注明技术专家的工作单位。

5.4.6.2 对于多场所审核，审核计划中应描述清楚多场所审核的安排，包括场地地址、距离总部的距离、审核时间、路途时间。

5.4.6.3 现场审核应安排在认证委托人的生产或服务处于正常运行时进行。

5.4.6.4 现场审核开始之前，应将审核计划提交给认证委托人并经其确认。如需要临时调整审核计划，应经双方协商一致后实施。

5.5 实施审核

5.5.1 审核组应按照审核计划实施审核，并采用中文记录审核过程，可使用图片、音像等作为补充材料。

5.5.2 审核组应会同认证委托人召开首、末次会议，认证委托人的最高管理者（因特殊原因不

能参加的，应授权高级管理层其他成员）、数据存储安全管理体系相关职能部门负责人应参加会议，缺席应记录理由。审核组应保留首、末次会议签到记录。

5.5.3 发生下列情况时，审核组应向本机构报告，经同意后终止审核：

（1）认证委托人对审核活动不予配合，审核活动无法进行；

（2）认证委托人实际情况与申请材料有重大不一致；

（3）其他导致审核程序无法完成的情况。

5.6 初次认证

5.6.1基于ISO/IEC 27040的数据存储安全管理体系审核时应采用文件调查和现场调查的方式，包括查阅文件和记录、询问工作人员、现场观察，必要时访问顾客和利益相关方、企业诚信行为调查等。 基于数据存储安全管理体系初次审核通常由第一阶段审核和第二阶段审核两个阶段组成。第一阶段审核可分为非现场审核或现场审核，一阶段审核通常包括对文件审核的进一步确认。

5.6.2 第一阶段审核

第一阶段审核的目的是通过对组织基于数据存储安全管理体系涉及的关键活动、方针、目标及管理制度等的策划情况来了解组织的基于数据存储安全管理体系建立情况，了解组织对审核准备的状态，为策划第二阶段审核提供关注的重点。

5.6.2.1 申请方符合以下条件时，第一阶段审核可以不在申请方现场进行：

（1）申请方已获标创公司颁发的其他有效认证证书，标创公司已对申请方的运作情况已了解；

（2）申请方提交的文件和资料充分，内容详实，通过文件和资料审查可以达到第一阶段审核目的和要求；

如申请方不满足以上条件，或提交文件和资料不充分，第一阶段审核需要结合申请方现场审核确定相关信息。

5.6.2.2第一阶段审核主要关注以下内容：

（1）确认申请组织实际情况与管理体系成文信息描述的一致性，特别是体系成文信息中描述的产品和服务、部门设置和职责与权限、过程等是否与申请组织的实际情况相一致；

（2）审核申请组织有关人员理解和实施标准要求的情况，评价管理体系运行过程中是

否实施了内部审核与管理评审，以及管理体系的实施程度能否证明客户已为第二阶段做好准备；

（3）确认申请组织建立的管理体系覆盖的活动内容和范围、申请组织的关键活动过程和场所，以及应对措施和合规计划的策划情况；

（4）结合管理体系覆盖活动的特点识别对合规目标的实现具有重要影响的关键点，并结合其他因素，科学确定重要审核点；

（5）审查第二阶段所需资源的配置情况，与申请组织讨论确定第二阶段审核安排。

（6）了解认证委托人的情况，包括其活动、产品和服务、设施设备、运作以及适用的标准，评价客户现场的具体情况，并与客户的人员进行讨论，以确定第二阶段的准备情况

（7）审核认证委托人理解和实施ISO/IEC 27040标准的情况，特别是对数据存储安全管理体系关键绩效、重要因素、过程、目标和运行识别情况；

（8）收集关于客户的管理体系范围的必要信息，包括：适用的法律法规要求、确认认证委托人数据存储安全管理体系认证范围、体系覆盖范围内有效人数和场所；

（9）认证委托人的产品和服务符合相关法律法规及强制性标准的情况。

（10）审查第二阶段所需资源的配置情况，并与客户商定第二阶段的细节；

（11）结合管理体系标准或其他规范性文件充分了解客户的管理体系和现场运作，以便为策划第二阶段提供关注点；

5.6.2.3 为达到第一阶段审核的目的和要求，除下列情况外，第一阶段审核活动应在认证委托人现场实施：

（1）认证委托人已获本机构颁发的其他领域的有效认证证书，本机构已对认证委托人数据存储安全管理体系有充分了解；

（2）本机构有充足的理由证明认证委托人的生产经营或服务的过程简单，体系影响较小，通过对其提交文件和资料的审核可以达到第一阶段审核的目的和要求；

（3）认证委托人获得了经认可机构认可的其他机构颁发的有效的数据存储安全管理体系认证证书，通过对其文件和资料的审核可以达到第一阶段审核的目的和要求。

本机构应记录未在现场进行第一阶段审核的理由。

5.6.2.4 本机构应将认证委托人是否具备二阶段审核条件的结论告知认证委托人，包括所识别的需引起关注的、在二阶段可能被判定为不符合项的问题。

5.6.2.5在第一阶段审核中，如发现组织存在违反审核依据的情况，审核组将以《审核问题汇

总表》指出，在《审核问题汇总表》中问题没有得到有效处理前，不会进行第二阶段审核。确认《审核问题汇总表》中的问题得到纠正或需进入现场验证而不影响二阶段审核时，方可进行第二阶段审核；第一、二阶段审核的时间间隔不应超过 6 个月。

5.6.3 第二阶段审核

5.6.3.1 第二阶段审核的目的是评价认证委托人数据存储安全管理体系的实施情况，包括对ISO/IEC 27040标准要求的符合性和体系的有效性。

5.6.3.2 第二阶段审核涉及受审核方申请范围内所有的产品、过程和职能部门。对于多场所，根据抽样原则确定审核场所。第二阶段审核至少覆盖以下内容：

（1）认证委托人数据存储安全管理体系与ISO/IEC 27040标准的符合情况及证据；

（2）依据数据存储安全管理体系关键绩效、目标和指标，对绩效进行的监视、测量、报告和评审；

（3）认证委托人实施数据存储安全管理体系的能力以及在符合适用法律法规要求方面的绩效；

（4）认证委托人过程的运作控制；

（5）在第一阶段审核中识别的重要审核点的过程控制的有效性；

（6）认证委托人的内部审核和管理评审是否有效；

（7）针对认证委托人数据存储安全管理体系方针的管理职责；

5.7 监督活动

5.7.1 本机构应对获证组织进行有效跟踪，包括依据审核方案对获证组织开展的监督审核，以确认获证组织数据存储安全管理体系与ISO/IEC 27040标准的持续符合性和运行的有效性。监督的目的是验证获证组织管理体系是否持续满足认证标准要求。监督审核分为定期监督审核和非定期监督审核。 获证组织的认证证书有效期通常为三年。证书有效期内，标创公司定期对获证组织进行两次监督审核，第一次监督审核自初次认证二阶段审核结束日期/再认证审核结束日期 12 个月内进行；第二次监督审核在第一次监督审核后 12 个月内进行，最长可以放宽到两次监督审核间隔 15 个月（原则上不能超过一个日历年）。 基本程序参照初次现场审核进行，监督现场审核时，认证范围覆盖的产品生产或服务活动应在正常运行，因市场、产品季节性等原因在每次监督审核时难以覆盖所有产品的，在认证证书有效期内的监督审核需覆盖认证范围内的所有产品，否则将缩小相应认证范围。根据监督审核结果，标创公司 做

出保持、暂停、撤销认证证书和缩小认证范围的决定。必要时，还需接受非例行监督审核或国家认监委/国家认可委实施的稽查和确认审核以及认证监管部门的稽查。

5.7.2 每次监督审核应尽可能覆盖认证范围内的有代表性的生产/服务过程；并确保在认证证书有效期内的监督审核覆盖认证范围内的所有代表性的生产/服务过程。

5.7.3 监督审核应重点关注获证组织的变更以及数据存储安全管理体系绩效的持续改进，获证组织在监督审核之前，应进行年度内部审核和评价，每次监督审核的内容主要包括：

（1）内部审核和管理评审是否规范和有效；

（2）对上次审核中确定的不符合项采取的纠正措施及效果；

（3）数据存储安全管理体系在实现获证组织目标和数据存储安全管理体系预期结果方面的有效性；

（4）为持续改进而策划的活动的进展；

（5）持续的运作控制；

（6）任何变更；

（7）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；

（8）数据存储安全管理体系相关投诉的处理。

5.7.4 监督审核的时间应根据获证组织当前情况（如有效人数）确定，不少于依据附录A所确定的初次认证审核时间的1/3(如果计算后结果包括小数，宜将其调整为最接近的半人日数（如：将 5.3 个审核人日调整为 5.5 个审核人日，5.2 个审核人日调整为 5 个审核人日）)。

5.7.5 符合下列条件时，保持认证资格：

（1）在每次监督审核前，组织按要求实施了有效的内审和评价；

（2）在认证证书有效期内，组织按期接受监督审核，其管理体系符合认证标准要求，或在认证证书有效期内，组织按期接受监督审核，其管理体系基本符合认证标准要求，对发生的不合格项能制定纠正措施计划，且在规定时间内有效完成；

（3）仅就获准认证的范围做出管理体系合格的声明，确保不采取误导的方式使用认证证书、标志或《审核报告》中任何一部分内容，对认证的宣传符合相关要求且未损坏标创公司的声誉；

（4）获证组织及时向 标创公司提供管理体系重大变动的信息和资料，及时提供发生的重大事故信息，提供的信息真实有效；

（5）遵守《认证合同》有关规定，包括按时缴纳认证费用；

（6）认证范围覆盖的产品、服务或活动符合法律法规要求。

5.7.6 在证书有效期内，获证组织的法定代表人、组织机构、管理体系文件及所覆盖的产品发生变化，或者发生与体系有关的事故等，应及时通报 标创公司。

（1）在认证证书有效期内，获证组织若发生了诚信相关或用户严重投诉，或因上述原因被主管部门查处、媒体曝光时，标创公司 将视情况做出暂停或撤销认证证书的决定。

（2）下列情况时，标创公司 将对获证组织进行提前较短时间通知或不通知的非定期审核：

- 国家认监委（CNCA）对标创公司提出相应要求时；
- 收到对获证组织投诉；
- 获证组织的管理体系和过程发生重大变更或影响管理体系绩效的较大以上事故或严重违法行为，可能影响体系正常运行；
- 对因管理体系运行存在不符合被暂停的组织进行追踪；
- 根据收集到的获证组织信息，公司认为有必要时。

非定期审核，不需要获证组织支付审核费用。标创公司 将视情况做出保持、暂停、撤销认证证书或缩小认证范围的决定。

5.8 再认证

5.8.1 获证组织拟继续持有认证证书的，应至少在认证证书到期前3个月向本机构提出再认证申请，逾期则按初次认证申请处理。认证证书到期前，应完成再认证审核的全部程序并做出认证决定，使新的认证周期在上一个认证周期结束时已经生效。如果因为获证组织原因导致在上一个认证有效期终止时未能做出认证决定的，认证证书自然到期失效。

5.8.2 本机构应依据审核方案实施再认证审核，以判断获证组织的数据存储安全管理体系作为一个整体与ISO/IEC 27040持续符合性和运行的有效性。

5.8.3 再认证审核应在获证组织现场进行，并应在认证证书到期前完成，在认证到期后，如果认证组织在 6 个月内配合完成未尽的再认证活动如：接受再认证审核、按期关闭不符合、按要求更新行政许可文件等，则可以恢复认证，作出更新认证证书的决定，否则应至少进行一次第二阶段审核才能恢复认证，作出更新认证证书的决定。证书失效期间组织的管理体系认证为无效状态。针对再认证项目作出更新认证的决定，还应考虑认证周期内的体系评价结果和认证使用方的投诉。证书的生效日期应不早于再认证决定日期，终止日期应基于上一个认证周期。再认证审核的内容至少应包括：

（1）结合其内部环境和外部环境的变化情况，确认获证组织数据存储安全管理体系有效性及认证范围的持续相关性和适宜性；

（2）数据存储安全管理体系绩效持续改进的证实；

（3）数据存储安全管理体系在实现获证组织目标和数据存储安全管理体系预期结果方面的有效性。

5.8.4 再认证审核策划时应考虑获证组织最近一个认证周期内的数据存储安全管理体系绩效，包括调阅以往的监督审核报告。

5.8.5 再认证审核的审核时间应按5.4.2的要求，根据获证组织当前情况（如有效人数）来确定，不少于依据附录所确定的初次认证审核时间的2/3(如果计算后结果包括小数，宜将其调整为最接近的半人日数（如：将 5.3 个审核人日调整为 5.5 个审核人日，5.2 个审核人日调整为 5 个审核人日）)。

5.8.6再认证审核的目的是确认管理体系作为一个整体的持续符合性与有效性，以及认证范围的持续适宜性。再认证审核程序与初次认证第二阶段审核程序一致，当管理体系及获证组织的内部和外部环境无重大变更时，再认证审核不需要第一阶段审核。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）有重大变更时，再认证审核需要安排第一阶段审核。

5.8.7 当获证组织申请利用再认证审核来扩大认证范围时，标创公司将对扩大认证范围的申请进行评审，通过现场审核后，做出能否予以扩大的决定。

5.8.8 对于再认证项目所有对应的认证范围应有生产现场。现场审核时，因市场、产品季节性等原因造成部分认证范围无生产现场的，审核组将建议缩小相应认证范围。在极个别特殊情况下（例如自然灾害）下，如果标创公司因不可抗力无法及时对某个获证组织实施再认证并换发认证证书，可延长其认证证书有效期。

当再认证获得批准后，颁发新的认证证书之日起，旧版认证证书将被撤销失效，再认证期间，请客户考虑使用旧版认证证书的风险。

5.9 特殊审核

5.9.1 扩大认证范围

对于已授予的认证，本机构应对扩大认证范围的申请进行评审，并确定任何必要的审核活动，以做出是否可予扩大的决定。这类审核活动可以结合监督审核同时进行。

5.9.2 提前较短时间通知的审核

为调查投诉、事故、对变更做出回应或对被暂停的客户进行追踪，可能需要在提前较短时间或不通知获证组织的情况下进行审核：

（1）本机构应说明并使获证组织提前了解将在何种条件下进行此类审核；

（2）由于获证组织缺乏对审核组成员的任命表示反对的机会，本机构应在指派审核组时给予更多的关注；

（3）获证组织在国家监督抽查中被查出不合格时，自监管部门发出通报后，本机构应对该组织及时实施监督审核。

5.10 不符合项纠正、纠正措施及其验证

5.10.1 对审核中发现的不符合项，本机构应要求认证委托人在规定的时限内进行原因分析，采取相应的纠正措施。

审核组采用抽样的方法，通过交谈、调阅文件与记录以及查看现场等方式，收集受审核方管理体系运行证据。如发现组织存在违反审核依据的情况，审核组将视问题的严重程度及其产生的影响，出具《不合格报告》，不符合严重程度分为：一般或严重。不合格最长关闭期限不超过 90 日，严重不符合不超过 6 个月。如果未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，则应拒绝其认证注册，或者重新实施第二阶段审核。

注 1：严重不合格项：影响管理体系实现预期结果的能力的不符合。如缺少或未能实施和保持管理体系标准的一个或多个要求，可能表明存在系统性失效，或根据获得的客观证据，足以怀疑组织管理体系绩效或过程控制可信性的审核发现。

注 2：一般不合格项：不影响管理体系实现预期结果能力的不合格项，但可能发展为严重不合格项的审核发现，如：

1）单个或孤立地缺少或未能实施和保持管理体系标准中某一项条款的要求，但其后果对组织的管理体系尚未构成严重影响；

2）在实施中未执行或偏离管理体系标准的要求，但其后果对组织的管理尚未构成严重影响；

3）违反组织有关文件要求，进而没有达到管理体系标准中某一项条款的要求。

（2）审核末次会议前，审核组将与受审核方负责人进行沟通。在末次会议上，确认不合格、宣布审核结论，并明确对不合格纠正措施的实施要求。

（3）现场审核结论包括“同意推荐认证注册”、“推迟推荐认证注册”或“拒绝推荐认证注册”三种。对审核中发现的不合格，受审核方应采取纠正措施，并经审核组验证。验证的方式有书面

验证和现场验证两种。验证合格后，审核组方能将《审核报告》及相关资料报 标创公司， 提交技术委员会审议。对于因受审核方原因，未能在规定期限内完成纠正措施的，审核组长可以修改审核结论。

当发生以下情况时，审核组将会终止审核：

（1）受审核方对审核活动不予配合，审核活动无法进行；

（2）受审核方的管理体系有重大缺陷，不符合标准的要求；

（3）发现受审核方体系运行存在重大问题或有其他严重违法违规行为；

（4）受审核方实际情况与申请资料有重大不一致；

（5）其他导致审核程序无法完成的情况。

5.10.2 本机构应对认证委托人所采取的纠正措施的有效性进行验证。认证委托人可以针对轻微不符合项制定纠正措施计划，由本机构在下次审核时验证。

5.10.3 严重不符合项的验证时限应满足以下要求：

（1）初次认证：在二阶段审核结束之日起6个月内完成；

（2）监督审核：在审核结束之日起3个月内完成；

（3）再认证：在审核结束之日起1个月内完成。

5.10.4 对于认证委托人未能在规定的时限内完成对不符合项所采取措施的情况，本机构不应做出授予认证、保持认证或更新认证的决定。

5.11 审核报告

5.11.1 本机构应就每次审核向认证委托人提供书面的审核报告。审核组长应对审核报告的内容负责。

5.11.2 审核报告的内容应准确、简明和清晰，反映认证委托人数据存储安全管理体系的真实状况，描述对照ISO/IEC 27040标准的符合性和有效性的客观证据信息，及对认证结论的推荐意见。

5.11.3 审核报告至少应包括或引用以下内容：

（1）本机构名称；

（2）认证委托人的名称和地址及其代表；

（3）审核类型（例如初次、监督、再认证或其他类型审核）；

（4）结合、联合或一体化审核情况（适用时）；

（5）审核准则；

（6）审核目的及其是否达到的确认；

（7）审核范围，特别是标识出所审核的组织、职能单元或过程，以及审核时间；

（8）任何偏离审核计划的情况及其理由；

（9）任何影响审核方案的重要事项；

（10）审核组成员姓名、身份及任何与审核组同行的人员；

（11）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；

（12）应描述与审核类型的要求一致的审核发现、审核证据（或审核证据的引用）以及审核结论，重点反映认证委托人主要产品和服务提供过程与控制情况、内部审核和管理评审的过程、所取得的绩效，认证委托人实际情况与其预期目标之间存在的差距和改进机会；

（13）行政监管部门在安全生产方面抽查的不合格情况，及相关原因分析和整改措施的有效性（适用时）；

（14）上次审核后发生的影响认证委托人数据存储安全管理体系的重要变更（适用时）；

（15）认证委托人对认证证书和认证标志的使用进行着有效的控制（适用时）；

（16）对以前不符合采取的纠正措施有效性的验证情况（适用时）；

（17）已识别出的任何未解决的问题；

（18）说明审核基于对可获得信息的抽样过程的免责声明；

（19）审核组的推荐意见以及对认证范围适宜性的结论。

5.11.4 本机构应保留用于证实审核报告中相关信息的证据。

5.11.5 本机构应将审核报告提交认证委托人。

5.11.6 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工作情况形成报告，本机构应将此报告提交给认证委托人。

5.12 认证复核、认证决定

5.12.1 本机构应在对审核报告、不符合项的纠正措施及验证情况和其他信息进行认证复核、综合评价的基础上，做出是否准予认证注册的决定，并书面通知受审核方。认证复核人员需要具备相应质量管理体系或环境管理体系或职业健康安全管理体系等领域注册类管理体系审核员的能力，认证决定人员应为本机构管理控制下的专职认证人员，并不得为审核组成员，能力应满足关于本机构资质审批的相关要求。认证决定过程不得外包，认证决定须由中华人民共和国境内

的工作人员做出。

5.12.2 本机构安排认证复核人员对于整个认证过程中形成的证据进行档案复核，确认认证审核过程及审核结论的公正性、有效性、真实性、完整性及充足性。

5.12.3 本机构安排认证决定人员对于基于认证复核人员的复核结果，对于关键内容进行二次评审，最终作出认证决定，关键内容至少包括：

a）审核组提供的信息足以确定认证要求的满足情况和认证范围；

b) 对于所有严重不符合，认证机构已审查、接受和验证了纠正和纠正措施：

c) 对于所有轻微不符合，认证机构已审查和接受了客户对纠正和纠正措施的计划。

5.12.4 本机构应有充分的证据确认认证委托人满足下列条件时，做出授予、更新、扩大认证范围的决定：

（1）5.1.2中的认证条件；

（2）对于严重不符合，已评审、接受并验证了纠正措施的有效性；对于轻微不符合，已评审、接受了认证委托人的纠正措施或计划采取的纠正措施；

（3）认证委托人的数据存储安全管理体系总体符合ISO/IEC 27040标准要求且运行有效；

（4）认证委托人按照认证合同规定履行了相关义务。

（5）申请组织已有效实施内部审核和评价；

（6）管理体系符合认证标准要求且运行有效，审核中未发现不合格，或管理体系基本符合认证标准要求，存在的不合格项在规定的时限内关闭（最迟90个工作日，严重不符合不超过6个月），且纠正措施和（或）纠正能够为审核组接受；

（7）认证范围覆盖的产品、服务或活动符合法律法规要求；

（8）审核报告应符合要求，审核组提供的审核报告及其他信息能够满足作出认证决定所需要的信息。

拒绝认证的条件

当认证组织不能满足认证要求时，即构成拒绝条件，包括但不限于：

（1）针对不合格项，未按期限有效关闭；

（2）提供虚假的认证信息；

（3）认证活动存在公正性问题；

（4）行政许可证明文件失效；

（5）不履行认证合同义务；

（6）受审核方的管理体系有重大缺陷，不符合标准的要求；

（7）发现受审核方存在重大诚信问题。

5.12.5 初次认证审核的认证决定应在现场审核后6个月内完成。否则应在推荐认证注册前再实施一次第二阶段审核。

5.12.6 再认证审核的认证决定应在上一认证周期认证证书到期前完成，否则应在推荐认证注册前再实施一次第二阶段审核。

5.12.7 认证委托人不能满足5.12.4要求的，本机构应将在《不批准认证注册通知书》中说明原因告知并说明其未通过认证的原因。

5.12.8 对于监督审核，本机构在满足下列条件时，可根据审核组长的肯定性结论保持对获证组织的认证：

（1）监督审核未发现严重不符合项及其他可能导致认证资格暂停、撤销的情况；

（2）获证组织认证信息未发生变更，不存在扩大、缩小认证范围的情况；

（3）本机构建立了监督审核的监视机制并予以实施，可确保监督审核活动的有效性。

6 认证证书和认证标志

6.1 总则

6.1.1 本机构应制定相应管理制度，要求获证组织正确使用数据存储安全管理体系认证证书和认证标志，以满足认证证书和认证标志相关管理规定。

6.1.2 获证组织可在认证有效期内使用数据存储安全管理体系认证标志，并接受本机构的监督管理。

6.1.3 获证组织应当在广告等有关宣传中正确使用数据存储安全管理体系认证标志，不得在产品上标注数据存储安全管理体系认证标志，只有在注明获证组织通过数据存储安全管理体系认证的情况下方可在产品的包装上标注数据存储安全管理体系认证标志。

6.1.4 本机构发现获证组织未正确使用认证证书和认证标志的，应当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 本机构应及时向认证决定符合要求的组织出具认证证书，认证证书的签发日期不应早于做

出认证决定日期。

6.2.2 数据存储安全管理体系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，再认证证书有效期的起算日期不得晚于最近一次有效认证证书的截止日期。

6.2.3 对每张数据存储安全管理体系认证证书应赋予一个认证证书编号。

6.2.4 认证证书在中华人民共和国境内使用的，证书使用的语言至少应包括中文。

6.2.5 认证证书的信息应真实、准确，不产生误导，并至少包含以下内容：

（1）获证组织名称、统一社会信用代码、注册地址、认证范围所覆盖的经营地址。若认证的数据存储安全管理体系覆盖多场所，应表述认证所覆盖的所有场所的地址信息；

注：认证证书中可不包括临时场所，当在认证证书上展示临时场所时，应注明这些场所为临时场所。

（2）获证组织数据存储安全管理体系所覆盖的产品、活动、服务的范围；包括每个场所相应的认证范围，且没有误导或歧义（适用时）；

（3）认证依据的认证标准ISO/IEC 27040所采用的当时有效版本的完整标准号；

（4）证书签发日期和有效截止日期，证书应注明：获证组织必须定期接受监督审核并合格此证书方可继续有效的提示信息。

（5）证书编号（或唯一的识别代码）；

（6）本机构名称、地址；

（7）认证标志、相关的认可标识及认可注册号（适用时）；

（8）证书信息及证书状态的查询途径。

6.2.6 认证机构对获得认证资格的申请方颁发认证证书，准予使用认证标志。认证证书中的表述审核标准采用ISO/IEC 27040标准。

6.2.7 认证标志为认证机构所有，获证组织应得到授权后方可使用。

6.2.8 认证机构对认证证书和认证标志的使用和展示进行监控，对于获证组织在广告、项目介绍等形式中对认证结果的不正确的引用，或者对认证证书或认证标志的误导性使，认证机构应视情况采取处置措施公布违规行为以及进一步采取法律措施等措施进行处理。 用

6.2.9 认证证书和认证标志的使用

（1）获证组织应对认证证书和认证标志的使用进行管理。认证证书的正确使用方法是：在宣传、投标等活动中展示认证证书，也可在文件、信签、广告和有关宣传材料上影印认证证书，使用必须完整，不得变形使用。

（2）获证组织不得变造、转让甚至非法买卖认证证书，也不得在知情的前提下容许他人或组织利用本组织的认证证书伪造、变造或冒用认证证书。

（3）认证证书/标志的使用者必须是认证证书（特别是有主/子证书及附件的情况）所载明的认证组织（即在证书及其附件中所列出的获证组织名称），除此之外其他任何单位不得使用该认证证书/标志。拥有认证证书/标志使用权的组织，应在其认证证书限定的审核地址及其过程等认证证书所明示的范围内使用，不得超出认证证书中限定的各自范围。有关方错误使用认证证书/标志带来的一切法律责任由使用者承担。

［例 1：仅集团公司总部单独获证的，集团公司下属分/子公司无权使用该证书（包括宣传、投标等活动）；同样，集团公司总部和集团公司下属的分/子公司 A 获证，集团公司下属的分/子公司B或其他分/子公司均无权使用该证书（包括宣传、投标等活动）；当集团公司总部与集团公司下属的分/子公司 A 的认证范围不一致时，集团公司总部与分/子公司 A 应仅在认证证书限定的各自范围内使用。］

（4）获证组织不得利用管理体系认证证书和相关文字、符号，误导公众认为其产品、服务通过认证。获证组织的管理体系发生重大变化时，应当向标创公司申请变更，未变更或者经标创公司调查发现不符合认证要求的，不得继续使用该认证证书。

（5）标创公司 拥有认证标志的所有权，并授权获证组织在认证范围和认证有效期内按照本文件的规定使用认证标志。获证组织拥有认证标志使用权，使用前须经标创公司对其使用方式进行认可、加以备案，未经标创公司允许，不得转让认证标志使用权。

（6）获证组织不得将认证标志用在产品上或产品包装之上，或以任何其他可解释为表示产品符合性的方式使用。

（7）获证组织可以将认证标志用在网页、宣传品、杂志、书籍、广告、促销材料、名片、投标书等，不允许将认证标志用于检测、校准或检验的报告或证书。可以采用印刷、图文和印章等使用方式，但应保证认证标志的完整，可按比例放大或缩小，但应确保认证标志的颜色与认证机构的徽标颜色一致并清晰可辨。当使用符号或标徽时，宜充分注意避免在宣传认证结果时损害认证机构的声誉。

（8）缩小认证资格的组织在缩小的范围内应立即停止任何关于获得标创公司认证的宣传，并应修改所有的广告材料。

（9）获证组织认证资格被撤销时，应立即停止任何关于获标创公司认证的宣传，并应

立即停止在网页、宣传品、杂志、书籍、广告、促销材料、名片、投标书等其他材料上继续使用认证标志。

（10）当获证组织因认证标志引起法律诉讼时，应及时通告 标创公司。

（11）必要时，标创公司 将与获准认证的组织协商制定对认证标志使用的其他要求，并形成相关文件。

（12）获证组织可以在产品包装上、附带信息及其他材料中声明组织的管理体系通过认证，但声明不应暗示产品、过程或服务得到了认证。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，型号标签或铭牌被视为产品的一部分。附带信息的判别标准是其可分开获得或易于分离，如产品合格证、产品使用说明书等。其他材料包括网页、宣传品、杂志、书籍、广告、促销材料、名片、投标书等。

（13）标创公司有权对获证组织使用认证证书和认证标志的情况进行监督，一旦发现获证组织有错误使用认证证书和认证标志现象，可以责成其采取纠正措施，并视情节轻重采取撤销其认证证书的措施，也可以上报国家认证认可监督管理委员会进行处理。

6.3 认证标志

本机构自行制定的认证标志的式样、文字和名称，不得违反法律、行政法规的规定，不得与国家推行的认证标志相同或者近似，不得妨碍社会管理，不得有损社会道德风尚。

获得认可后可使用认证标志，获证组织须在与标创公司签署有关使用认证标志的协议后才可以使用认证标志，认证标志应与认证机构的认证标志并列使用。

获证组织不得将认证标志用于产品、产品包装及附带信息上，可用于网页、宣传品、杂志、书 籍、广告、促销材料、名片、投标书等其他材料。

7.认证证书状态管理

7.1 总则

本机构应制定认证资格有效、暂停、撤销和注销的文件化的管理制度，并遵照执行，不得随意暂停、撤销和注销认证资格。

7.2 认证证书有效管理

通过认证决定的获证组织，本机构颁发认证证书，对于初审、再认证类型，在认证颁发后的次月10号，将认证证书报送国家认监委，并将认证证书信息通过本机构官网予以公示。

7.3 认证资格的暂停

7.3.1 获证组织有以下情形之一的，本机构应在调查核实后的2-5个工作日内暂停其认证资格，并保留相应证据：

（1）数据存储安全管理体系持续或严重不满足认证要求的；

（2）不满足数据存储安全管理体系适用的法律法规要求，且未采取有效纠正措施的；

（3）受到与安全生产相关的行政处罚；

（4）发生较大或重大事故，反映获证组织数据存储安全管理体系运行存在重大缺陷的；

（5）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的；

（6）持有的与数据存储安全管理体系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的；

（7）不能按照规定的时间间隔接受监督审核的；

（8）未按相关规定正确引用和宣传获得的认证资格和有关信息，包括认证证书和认证标志的使用，造成严重影响或后果的；

（9）不承担、履行认证合同约定的责任和义务的；

（10）被有关行政监管部门责令停业整顿的；

（11）发生与数据存储安全管理体系相关的重大舆情；

（12）主动请求暂停的；

（13）其他应暂停认证资格的。

7.3.2 本机构可根据暂停的原因和性质确定暂停期限，暂停期限最长不得超过6个月。

7.3.3 暂停期间，如获证组织采取有效的纠正措施，造成暂停的原因已消除的，本机构应恢复其认证资格，并保留相应证据。

7.3.4 暂停期为1个月到6个月，暂停期可至相关单位作出许可决定之日。标创公司 将向获证组织发出《暂停资格通知书》、同时向行业管理部门上报相关信息并向社会公告。获证组织应按通知书规定的有关要求执行，在暂停期间，获证组织的管理体系认证暂时无效。获证组织接到《暂停资格通知书》后，在规定时间内完成以上情况的纠正和/或纠正措施，经标创公司验证，必要时，经指定的审核组现场验证、证明已满足要求，将恢复其认证注册资格。

7.4 认证资格的撤销

获证组织有以下情形之一的，本机构应在获得相关信息并确认后2-5个工作日内撤销其认证资格，并保留相应证据：

（1）被注销或撤销法律地位证明文件的；

（2）被国家企业信用信息公示系统和“信用中国”列入严重违法失信名单的；

（3）认证资格的暂停期限已满，但导致暂停的问题未得到解决或有效纠正的；

（4）因获证组织违规造成重大产品和服务等事故的；

（5）有其他严重违反数据存储安全管理体系相关法律法规行为，受到相关行政监管部门处罚的；

（6）数据存储安全管理体系没有运行或者已不具备运行条件的；

（7）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，或者本机构已要求其纠正但超过1个月仍未纠正的；

（8）其他应撤销认证资格的。

7.5 认证资格的注销

当获证组织部分认证范围无法满足规定要求时，可撤销部分认证范围；当获证组织全部认证范围无法满足规定要求时，撤销全部认证范围。标创公司向获证组织发出《撤销认证资格通知书》，并以公告形式公布，组织应交回认证证书。被撤销的认证证书信息，标创公司 将及时上报至国家认监委网站。

7.6 更换证书

出现下列情况之一时，重新更换认证证书

（1）在认证证书有效期内，出现下列情况之一的，应按照有关规定重新换证：

- 管理体系认证标准转换；
- 标创公司 名称、认证标志发生变化；
- 组织认证范围发生变化；
- 组织名称、地址和统一信用代码等认证证书信息发生变化。

（2）在管理体系认证标准变更的情况下，要安排进行审核，审核与认证决定通过后，重新换证，审核可结合年度监督或再认证进行。

（3）在获证组织体系认证范围变更时，获证组织应及时通知 标创公司，如变更的发生对体系产生了较严重的影响时，则需要重新进行审核，审核与认证决定通过后重新换证。

8. 申诉和投诉处理

8.1 为确保基于数据存储安全管理体系认证的公正性和工作质量，维护受审核方、获证组织与认证机构的权益，本机构应建立文件化的申诉和投诉处理制度，并遵照执行；认证委托人对认证决定有异议的，可以向本机构提出申诉；任何组织和个人对认证过程和决定有异议的，可以向本机构提出投诉。。

8.2 申诉和投诉的提交、调查和决定不应造成针对申诉人/投诉人的歧视。本机构对申诉人（投诉人）、申诉和投诉事项的信息应予以保密。

8.3 本机构应及时、公正、有效地处理申诉和投诉，采取必要的纠正措施。对申诉和投诉的处理决定，应由与申诉和投诉事项无关的人员做出，或经其审核和批准，并应在60日内将处理结果书面告知申诉人或投诉人。

8.4 认为本机构未遵守认证相关法律法规或本规则，并导致自身合法权益受到严重侵害的，可以直接向本机构所在地市场监管部门或国家认监委投诉。

8.5 投诉的处理

8.5.1 组织可向标创公司提出书面或口头投诉，书面提出的应在信封上注明“投诉”字样。

8.5.2 针对获证组织的投诉，标创公司 将投诉事宜告知该获证组织，请其配合调查。

8.5.3 在 30 个工作日内，标创公司完成对投诉的调查和处理，并将调查和处理结果通知投诉方，如果组织对投诉处理结果不满意，可以向认证机构上级主管部门进行投诉。

8.5.4 标创公司 应与获证组织及投诉人共同决定是否应将投诉事项公开，并在决定公开时，共同确定公开的程度。

8.6 申诉的处理

8.6.1 申诉人对标创公司做出的不予认证、暂停或撤销其认证资格、扩大或缩小其认证范围等决定有异议时，在标创公司做出上述决定的三个月内，可以提出申诉。所有申诉必须以“申诉函”的形式书面正式提出，应在申诉材料的信封上注明“申诉”字样。

8.6.2 在接到申诉函后 10 个工作日内，标创公司 总经理负责授权组成申诉工作组，确保参与申诉处理过程的人员没有实施申诉涉及的审核，也没有做出申诉涉及的认证决定。

8.6.3 申诉的提出、调查和决定不应造成针对申诉人的任何歧视行为。

8.6.4 申诉工作组在 60 日内做出处理结果，将申诉的处理结果通知申诉方，并明确：如果对申诉处理结果不满意，可以向认证机构上级主管部门投诉。若认为认证机构未遵守认证相关法律法规或本规则并导致自身合法权益受到严重侵害的，可以直接向所在地认证监管部门或国家认监委投诉。

8.6.5 败诉方承担申诉/投诉过程中的一切费用。

9. 信息公开与报告

9.1 本机构应建立文件化的认证信息报告制度，并遵照执行。按照国家认监委关于认证信息上报的要求，按时上报认证相关信息，至少包括：

（1）上一年度工作报告；

（2）社会责任报告；

（3）认证计划及认证结果；

（4）认证证书的状态；

（5）其他应报告的信息。

9.2 本机构应至少在审核实施前，按要求将审核计划上报国家认监委相关网站，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。

9.3 本机构在颁发认证证书后，应在次月10日前，将认证结果相关信息报送国家认监委。

本机构应通过网站或者其他形式，向公众提供查询认证证书有效性的方式。

9.4 本机构应通过其网站或者其他方式公开暂停、撤销、注销认证证书的信息，暂停证书的，还应明确暂停的起始日期和暂停期限。本机构应在暂停、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。

9.5 信息沟通

获证组织应将管理体系相关信息及变更情况或其组织发生重大事故时应及时向标创公司通报，使公司能够对获证组织管理体系的变化及时做出响应，以确保认证管理的有效性；认证组织及其相关方可以向我公司索要必要的与认证相关的信息。

重大事故：指获证组织发生有关合规在其相应行业法规中定义为重大（较大）级别以上的，和（或）引起新闻媒体及社会关注的事故。

索要信息：包括认证机构运作涉及的地理区域、特定获证客户的认证证书状态、名称、相关的规范性文件、认证范围和地理位置、转换获得认可认证证书所必须的信息等。

9.5.1 获证组织管理体系信息通报的内容

（1）组织的法律地位、经营状况、组织状态或所有权等的变更；

（2）法定代表人、最高管理者、体系负责人等关键的决策、管理或技术人员的变更；

（3）取得的行政许可资格、强制性认证或其他资质证书变更；

（4）管理体系文件的变更；

（5）管理体系覆盖的活动范围变更

（6）管理体系和重要过程、设施设备的重大变更；

（7）生产经营或服务的工作场所，包括分场所的变更；

（8）相关机构（如与认证证书相关的分支机构等）的变更；

（9）其他方面的变更（如体系覆盖人数、联系信息等）；

（10）出现影响管理体系运行的其他重要情况；

（11）组织生产、销售的产品或提供的服务被质量或市场监管部门认定不合格，发生重大的与诚信方面的事故，以及与诚信相关的重大投诉及有关部门的处罚；

（12）与组织基于数据存储安全管理体系相关的法律法规的变化情况。

9.5.2 通报程序

（1）获证组织如发生以上管理体系信息通报中 1-9 项相关的变更时，要求在 10 个工作日内书面报告 标创公司，并提交相应的证明文件；标创公司 将根据变更的实际情况做出是否安排实施增加频次的监督审核或再认证。

（2）如果获证组织发生了管理体系信息通报中第 10 项的重大事故、重大投诉或处罚时； 要求在 5 个工作日内将相关情况书面报告 标创公司，标创公司 将根据重大事故或投诉的实际情况和认证认可有关规定做出相应处理。

（3）标创公司 同时将主动对上述涉及变更或发生重大事故的获证组织信息进行搜集与分类， 对可能影响认证注册资格保持的信息，由标创公司进行分析并提出：

（4）针对存在问题，实施增加频次的监督审核或再认证，确认事故是否与管理体系的运行直接相关，以确定是否需要暂停/撤销认证资格；

（5）直接暂停/撤销认证资格；

（6）特别提示：对于获证组织因未能主动报告重大事故、重大投诉及相关变更的，标创公司 将按照认证认可规定对组织的认证资格做出严格处理。

（7）自事故发生之日起，标创公司 负责在 10 天内将事故情况以及已/拟采取措施书面报告 CNAS。

（8）暂停/撤销认证资格的意见/建议由 标创公司技术委员会做出决定。

（9）获证组织应建立程序，对本组织管理体系变更及通报认证公司做出安排，包括指定负责本文件实施以及与标创公司沟通的人员。

9.5.3 索要信息的处理

（1）获证客户及相关方可通过标创公司网站（www. ovcc.co）查看标创公司公开信息，或通过在标创公司 网站（www. ovcc.co）的“证书查询”栏目、认监委网站（www.cnca.gov.cn），通过填报获证客户的名称或证书号查询相关索要信息。

（2）需要时，获证客户及相关方可联系标创公司客服人员，提出索要信息查询的书面申请，标创公司 根据获证客户及相关方的需求提供书面证明或公开相关信息。

10. 认证记录

10.1 本机构应建立文件化的认证记录、认证资料归档留存制度，记录认证活动全过程并妥善保存，归档留存时间为认证证书有效期届满或者被注销、撤销之日起2年以上。

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）审核方案；

（5）审核计划；

（6）首、末次会议签到表；

（7）现场审核记录；

（8）不符合项报告及验证记录；

（9）审核报告；

（10）认证决定记录。

10.3 在认证证书有效期内，认证活动参与各方签字或者盖章的认证记录、资料等，应保存具有法律效力的纸质版原件。签字或盖章的认证记录至少包括：

（1）认证申请书；

（2）认证合同；

（3）审核计划；

（4）首、末次会议签到表；

（5）不符合项报告及验证记录。

10.4 认证记录应使用中文，以电子文档的形式保存认证记录的，应采用不可编辑的方式。

11 其他

认证标准换版

本机构按照国家市场监管部门统一制订发布的ISO/IEC 27040标准的换版工作要求，执行落实标准的换版工作，确保组织能够及时获得新版标准认证。

12 认证收费说明

标创公司应严格执行国家有关主管部门的收费规定。

附录A

信息安全管理体系有效员工人数与审核时间的关系

在组织控制下工作的人员的数量	质量管理体系初次审核审核时间(审核人日， d)	环境管理体系初次审核审核时间(审核人日， d)	ISMS初次审核审核时间(审核人日， d)
1~10	1.5~2	2.5~3	5
11~15	2.5	3.5	6
16~25	3	4.5	7
26~45	4	5.5	8.5
46~65	5	6	10
66~85	6	7	11
86~125	7	8	12
126~175	8	9	13
176~275	9	10	14
276~425	10	11	15
426~625	11	12	16.5
626~875	12	13	17.5
876~1175	13	15	18.5
1176~1550	14	16	19.5
1551~2025	15	17	21
2026~2675	16	18	22
2676~3450	17	19	23
3451~4350	18	20	24
4351~5450	19	21	25
5451~6800	20	23	26
6801~8500	21	25	27
8501～10700	22	27	28
>10700	沿用以上规律	沿用以上规律	沿用以上规律

注 1：表中的人数宜视为连续变化的，而不是阶梯式变化的。即如果画成曲线图，线段的起点宜来自表格上一栏的值，并以表格每栏值为每段的终点。曲线（以中级复杂程度为例）的起点是人数为1时对应1.5天。对非整数审核人日的处理，如果计算后结果包括小数，宜将其调整为最接近的半人日数。

注 2：人数超过10700人时对审核时间的计算。该审核时间宜遵循表中的递进规律，与该表保持一致。

注 3：有效人数，包括认证范围内涉及的所有全职人员，原则上以组织的社会保险登记证所附名册等信息为准。

注4：对非固定人员（包括季节性人员、临时人员和分包商人员）和兼职人员的有效人数核定，可根据其实际工作小时数予以适当减少或换算成等效的全职人员数。

文件修订记录

序号	章节	版本号	更改内容	修改方式	更改时间
1	全部	A/0	/	新版发布	2024年6月1日
2	全部	B/0	依据《国家认监委关于加强认证规则管理的公告2025年第9号》进行修订改版	换版	2025年4月10日