大语言模型供应链安全管理体系认证规则



北京赛西认证有限责任公司

（原中国电子技术标准化研究所认证中心）

2026-05-15 发布　　2026-05-15 实施

目　录

前　言 I
1 总则 1
1.1　目的 1
1.2　适用范围 1
1.3 主要依据文件 1
1.4 认证准则 1
1.5 术语说明 1
2　申请方条件 2
3　认证要求 2
3.1 认证流程 2
3.2 认证申请 3
3.3 审核方案策划及审核策划 3
3.3.1 审核方案 3
3.3.2 审核时间 3
3.3.3 多场所抽样 4
3.3.4 组建审核组 4
3.3.5 审核计划 5
3.4 实施审核 5
3.5　初次认证审核 5
3.5.1　第一阶段审核 5
3.5.2　第二阶段审核 7
3.6 保持认证 7
3.6.1 保持认证的条件 7
3.6.2 监督审核 8
3.6.3 再认证审核 8
3.6.4 特殊审核 9
3.7 审核报告 10
3.8 不符合纠正及验证 11
3.9 认证决定 11

3.10 证书有效期内的情况通报 12
3.11 认证要求的变更 13
4 认证标志和认证证书 13
4.1 认证标志 13
4.2 认证证书 13
4.2.1 认证证书内容 14
4.2.2 证书编号 14
4.3 认证标志和证书的使用 15
4.3.1 使用要求 13
4.3.2 使用申请 15
4.4 违规处理 16
5 暂停、撤销、注销认证的条件及程序 16
5.1 暂停 16
5.2 撤销 17
5.3 注销 18
5.4 公示 18
6 申诉、投诉 18
7 收费 18
8 其他 19
附录 1 国家认证认可监督管理委员会批文 20
附录 2 管理体系信息通报表 21
附录 3 CESI 认证业务联系方式 22
附录 4 认证证书样式 23
附录 5 审核时间 24

前 言

本认证规则由北京赛西认证有限责任公司制订并发布，版权归北京赛西认证有限责任公司所有，任何组织及个人未经许可，不得以任何形式全部或部分使用本规则。本规则的最终解释权归北京赛西认证有限责任公司所有。

本规则于 2025 年 9 月 1 日首次发布；。

2026 年 5 月 15 日，修订至 V1.1 版，主要是依据国家认监委 6 项管理体系认证规则对本规则进一步全面修订。

1 总则

1.1 目的

为保证北京赛西认证有限责任公司(以下简称赛西认证)有序、有效地实施大语言模型供应链安全管理体系认证工作，科学、公正地为所有申请方提供优良的管理体系认证服务，使申请方/受审核方/获证组织充分了解赛西认证的认证程序和有关规定，特制定本认证规则，并作为公开文件向申请方提供。

1.2 适用范围

本认证规则适用于赛西认证开展的大语言模型供应链安全管理体系认证工作，可为申请方/受审核方/获证组织进行管理体系认证/注册提供指导。

1.3 主要依据文件

《国家认监委关于加强认证规则管理的公告》（认监委公告 2025 年第 9 号）

GB/T 27021.1 合格评定 管理体系审核认证机构要求 第 1 部分：要求

GB/T 19011 管理体系审核指南

质量管理体系认证规则（CNCA-QMS-01:2025）

1.4 认证准则

大语言模型供应链安全管理体系认证的基本准则是 WDTA AI-STR-03 标准。

1.5 术语说明

根据认证过程的变化,本规则对申请认证组织使用了不同的称呼:

申请方：认证审核之前

受审核方：审核过程中及获证前

获证组织：获得管理体系认证证书后。

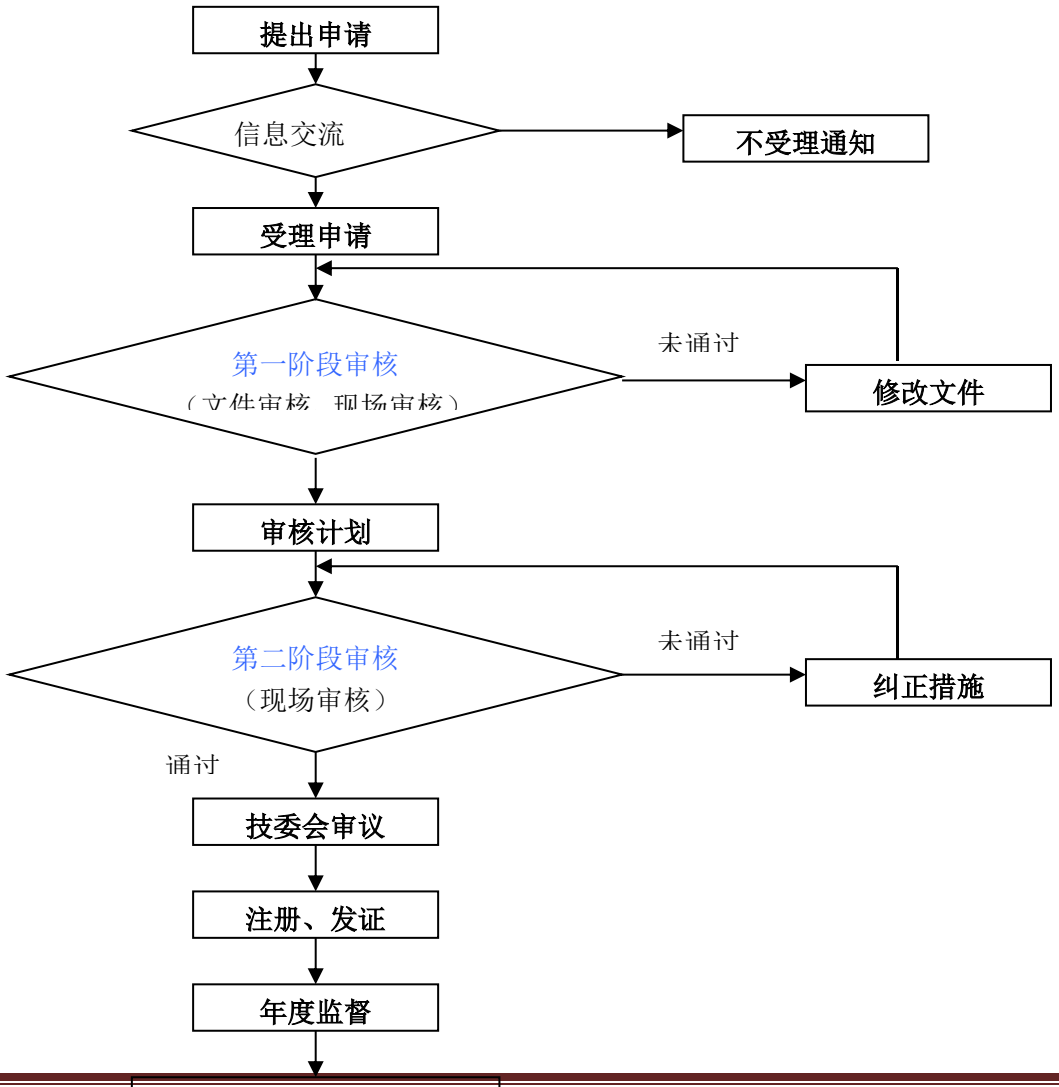
2 申请方条件

申请方应满足如下条件：

1) 取得法人资格(或其组成部分)，并处于有效期内；
2) 取得相关法规规定的行政许可(适用时)，并处于有效期内；
3) 已建立大语言模型供应链安全管理体系并运行满 3 个月，且已实施覆盖所有程序的内部审核和管理评审；
4) 当前未被行政监管部门责令停业整顿；
5) 当前未被列入国家企业信用信息公示系统和“信用中国”发布的严重违法失信名单。

3 认证要求

3.1 认证流程



3.2 认证申请

a. 申请方向赛西认证提出认证申请意向。

b. 赛西认证与申请方沟通并办理“申请书”及商谈采用的认证标准或文件。

c. 申请方向赛西认证提交管理手册及相应的程序文件以及有关的文件清单。

d. 赛西认证对认证申请进行评审，在确认申请认证有关的要求明确，且赛西认证有能力完成认证工作的前提下与申请方签订认证合同。

赛西认证在受理认证申请时，还将与申请方就体系覆盖产品、认证范围及“认证合同”等有关具体事宜进行协商。

认证费用应由申请方向赛西认证直接支付，不得通过第三方支付。特殊情况下，可以接受申请方的上级单位（如申请方所属的集团公司、 事业单位、社会团体或机关）或下级单位向赛西认证支付认证费用。

3.3 审核方案策划及审核策划

3.3.1 审核方案

根据申请信息及合同评审情况，赛西认证审核业务部门建立审核方案。初次认证的审核方案包括两阶段初次认证审核、获证后的监督审核和认证到期前的再认证审核。再认证的审核方案包括再认证审核、获证后的监督审核和认证到期前的再认证审核。

初次认证及再认证后的第一次监督审核在认证证书签发之日起 12 个月内进行。此后，监督审核间隔不超过 12 个月，且监督审核至少每个日历年（应进行再认证的年份除外）进行一次。如有特殊情况或在法律、法规要求下，将增加监督审核频次。

3.3.2 审核时间

审核时间包括现场的审核时间以及在现场审核以外实施策划、文件审核和编写审核报告等活动的时间。审核时间以人日计，1 人日为 8 小时。如果受审核方工作日的实际工作时间不足 8 小时，则需延长现场审核天数以满足审核时间要求。

附录 5 规定了审核时间，根据受审核方体系有效人数、体系复杂程度类型等因素，可能会适当调整审核时间。

每次审核的审核时间确定过程应形成记录，尤其是减少审核时间的理由，减少的审核时间不得超过附录B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%。如果审核人日计算后结果包括小数，宜将其调整为最接近的半人日数。

大语言模型供应链安全管理体系和其他管理体系实施结合审核的，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%。（注：对于市场监管总局(国家认监委)或认可机构有明确审核时间要求的管理体系，大语言模型供应链安全管理体系不能与其实施结合审核的，也不能通过结合审核的方式减少审核时间。）

3.3.3 多场所抽样

对受审核方涵盖相同活动、过程及复杂程度类型的多个相似场所可进行抽样审核，抽样数量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。

对多个非相似场所，则不进行抽样。初审和再认证审核逐一到各场所进行审核。监督审核抽取不少于30%的场所进行审核，且每次审核均包括中心职能部门。第二次监督审核选取的场所通常不同于第一次监督审核所选取的场所。

3.3.4 组建审核组

赛西认证审核业务部门根据实现审核目的所需的能力和公正性要求组建审核组，至少1名实施第一阶段审核的审核员应参加第二阶段审核，每个审核组应满足如下条件：

(1) 包括至少1名与受审核方所属认证业务范围相匹配的专业人员（专业领域审核员或技术专家）。非专业审核人员，不得实施专业过程的审核任务；

(2) 包括至少1名赛西认证的专职审核员，该专职审核员全程参与审核过程；

(3) 开展认证审核的所有审核员，除应取得国家承认的注册审核员资格外，还应取得机构评定的大语言模型供应链安全管理体系审核员资格；

(4) 必要时，审核组可配备技术专家，为审核组提供技术支持，技术专家不作为审核员实施审核，其审核时长不计入审核时间；

(5) 审核组如有实习审核员，需在正式审核员的指导下参加审核，不得独自开展审核，其审核时长不计入审核时间。

3.3.5 审核计划

现场审核应安排在受审核方的生产或服务处于正常运行时进行。

审核组根据受审核方管理体系和所涉及产品、活动、服务的特点制定审核计划，并将审核计划在现场审核前提交受审核方确认，受审核方如有异议可以提出，由赛西认证和受审核方协商调整后实施。

3.4 实施审核

3.4.1 认证审核需在受审核方的现场实施，包括初次认证审核以及认证周期内的每年度的监督审核、再认证审核和特殊审核。

3.4.2 审核组会同受审核方召开首、末次会议，受审核方的最高管理者、相关职能部门负责人应参加首、末次会议。受审核方的最高管理者不能参加首、末次会议的，应由获得书面授权的其他高级管理层成员参会。

3.4.3 审核组通过面对面访谈等形式，对受审核方的最高管理者在大语言模型供应链安全管理体系中发挥领导作用的情况进行重点审核，并保留现场图片/音像、审核记录等证明材料。最高管理者不熟悉组织自身的方针、目标，未亲自参与并推动大语言模型供应链安全管理体系实施的，认证审核应不予通过。

3.4.4 发生下列情况的，审核组应向赛西认证报告后终止审核：

1） 认证委托人对审核活动不予配合，审核活动无法进行；

2） 认证委托人的最高管理者或其授权的高级管理层成员，缺席首次会议或末次会议的；

3） 认证委托人实际情况与申请材料有重大不一致；

4） 其他导致审核程序无法完成的情况。

3.5 初次认证审核

管理体系的初次认证审核分为第一阶段审核和第二阶段审核。两个阶段审核时间间隔最短不应少于 5 日，最长不应超过 6 个月。如需要更长的时间间隔，应重新实施第一阶段审核。

3.5.1 第一阶段审核

3.5.1.1 第一阶段审核内容

第一阶段是通过了解受审核方所建立的管理体系和其对第二阶段的准备情况，确定其是

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。通常情况下，第一阶段审核活动在受审核方现场实施。

第一阶段审核包括以下内容：

a. 了解受审核方的情况，包括其活动、产品和服务、设施设备、工艺流程、现场运作以及适用的管理标准；

b. 评审受审核方大语言模型供应链安全管理体系文件，确认其与受审核方业务活动及产品和服务相吻合；

c. 确认受审核方申请信息和文件资料的真实性。审核受审核方的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、生产或服务过程等是否与受审核方的实际情况相一致；

d. 评价受审核方的运作场所和现场的具体情况，确定第二阶段审核的准备情况；与受审核方商定二阶段审核细节及重要审核点；

e. 收集关于受审核方的管理体系覆盖的活动内容和范围、过程和场所、体系范围内有效人数的必要信息；

f. 评价受审核方是否策划和实施了内部审核与管理评审，确认管理体系是否已运行并且超过 3 个月以及管理体系的实施程度能否证明客户已为第二阶段审核做好准备。对管理体系成文信息不符合现场实际、相关体系运行尚未超过 3 个月或者无法证明超过 3 个月，以及其他不具备二阶段审核条件的，不应实施二阶段审核。

第一阶段审核发现会以书面方式并告知受审核方，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。如需整改的，受审核方需按审核组要求完成整改。

当审核组通过第一阶段审核发现相关申请信息和文件资料存在虚假情况的，将终止认证活动。

3.5.1.2 第一阶段现场审核程序

1) 现场审核开始时，首先召开首次会议，审核组在首次会议上向受审核方说明审核目的、审核依据、审核覆盖范围和审核方法、明确受限制区域，确认审核计划，同时将可能引起审核中止的条件告知受审核方。如双方有不同意见，应协商解决。

2) 审核组根据审核计划及事先编制的审核核查单，采用会晤、访问、查阅文件记录、现场观察等方法，对受审核方的管理体系进行审核，取得客观证据，并记录审核结果。

3) 在审核期间，受审核方应予协助、配合，并保证：

a) 审核组能够查阅组织管理体系有关的文件资料和质量记录，包括原始记录；

b) 审核组能够进入与管理体系审核有关的场所；

c) 审核组能够与管理体系有关的人员进行访谈；

d） 提供审核组进行管理体系审核时所必需的设施和条件，并指定陪同人员。

4） 现场审核结束前，审核组应与受审核方负责人（或其代表）进行会晤，表明审核组第一阶段现场审核的意见。并召开末次会议，表明审核组现场审核的结论意见。

5） 在审核中发现的问题，由受审核方采取纠正措施，并在第二阶段审核前完成，审核组在第二阶段审核前或第二阶段现场审核时予以验证。

3.5.2 第二阶段审核

第二阶段审核的内容是对组织的管理体系实施的有效性进行评价。现场审核程序参见第一阶段要求。

第二阶段审核应在受审核方的现场实施，至少覆盖以下内容：

1） 受审核方大语言模型供应链安全管理体系与认证依据标准的符合情况及证据；

2） 依据大语言模型供应链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） 受审核方实施大语言模型供应链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） 受审核方大语言模型供应链安全管理体系管理过程的运作控制；

5） 受审核方的内部审核和管理评审；

6） 针对受审核方大语言模型供应链安全管理体系方针的管理职责等。

二阶段审核组现场审核结论包括下列三种情况

a. 不推荐注册；

b. 推荐注册；

c. 待纠正措施实施并验证确认符合要求后推荐注册。

受审核方如对结论意见有不同看法，与审核组不能达成一致时，审核组应专门加以记录并报告赛西认证。

对于现场审核结论，组长有最后决定权。

3.6 保持认证

3.6.1 保持认证的条件

保持获准认证/注册组织大语言模型供应链安全管理体系持续有效，应符合下列条件：

a. 获证组织的法律地位、资质持续符合国家的最新要求，认证范围内的法律地位文件和

资质持续有效；

b. 按赛西认证规定的周期和程序接受监督审核；

c. 认证证书、认证标志使用符合赛西认证的规定要求；

d. 按规定要求及时向赛西认证报告管理体系的变更情况；

e. 按规定交纳监督审核费用。

3.6.2 监督审核

赛西认证将通过监督审核对获证组织进行有效跟踪，获证组织的最高管理者需参与审核访谈，以确认获证组织大语言模型供应链安全管理体系与认证依据标准的持续符合性和运行的有效性。

监督审核重点关注获证组织的变更以及大语言模型供应链安全管理体系绩效的持续改进，监督审核的内容至少包括：

1) 内部审核和管理评审；

2) 对上次审核中确定的不符合采取的纠正措施及效果；

3) 大语言模型供应链安全管理体系在实现获证组织目标和大语言模型供应链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) 大语言模型供应链安全管理体系相关投诉的处理等。

3.6.3 再认证审核

认证合格证书有效期满前三个月，获证组织想要继续持有认证证书的，可提出再认证申请。赛西认证将依据审核方案实施再认证审核，再认证的程序与初次审核时的程序相同。

再认证审核在获证组织现场进行，并应在认证证书到期前完成。再认证审核的内容至少包括：

1) 结合其内部环境和外部环境的变化情况，确认获证组织大语言模型供应链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) 大语言模型供应链安全管理体系绩效持续改进的证实；

3) 大语言模型供应链安全管理体系在实现获证组织目标和大语言模型供应链安全管理

体系预期结果方面的有效性。

经全面再认证确认获证组织管理体系持续满足管理体系标准要求，赛西认证批准同意其延长，并更换证书。

3.6.4 特殊审核

3.6.4.1 扩大认证范围

扩大认证范围包括认证依据标准的扩大，也可包括过程（活动）的增加、产品范围、生产规模（场地、区域）的扩大。

3.6.4.1.1 扩大认证范围的条件

a. 获证组织申请扩大认证范围应在其法律地位文件和资质规定的范围内；

b. 获证组织的管理体系应覆盖申请扩大的认证范围，并符合认证标准要求；

c. 至少近一年来，获证组织在申请扩大认证范围内未发生重大事故和国家检查不合格。

3.6.4.1.2 扩大认证范围的程序

a. 获证组织需向赛西认证正式提交扩大认证范围的书面申请书和相关附件；

b. 赛西认证对获证组织的扩项申请进行评审，适用时获证组织应与赛西认证补充签署或修订认证合同，并按照规定补充缴纳认证费用；

c. 获证组织申请扩大认证范围所涉及的管理体系文件经审查已符合认证标准；

d. 对获证组织申请扩大认证范围所涉及的管理体系，赛西认证结合监督审核或按协议要求实施认证程序（如有规定，对简单的扩大认证范围可以不需要现场审核），对认证合格者按初审程序更换证书。

3.6.4.2 缩小认证范围

3.6.4.2.1 缩小认证范围的条件

如果组织在认证范围的某些部分持续地或严重地不满足认证要求，赛西认证将按照认证标准的要求缩小其认证范围，以排除不满足要求的部分，具体情况如下：

a. 获证组织的认证范围内部分产品范围、现场、区域、生产线、主要过程等不再继续符合认证标准和其他附加要求；或

b. 获证组织的认证范围内部分产品范围、现场、区域、生产线、主要过程等不愿再继续保持认证资格的。

3.6.4.2.2 缩小认证范围的程序

a. 获证组织向赛西认证正式提交缩小认证范围的书面申请书，并提供理由和证据；

b. 需要时，获证组织与赛西认证修订认证合同；

c.经赛西认证技术委会审定，认为获证组织在申请缩小认证范围不会对仍需保持的认证范围产生影响，报公司总经理批准，由公司总经理签署换发认证证书，但认证证书的注册号和有效期保持不变。

3.6.4.3 提前较短时间通知的审核

为调查投诉、体系相关事故、对变更做出回应或对被暂停的客户进行追踪等情形时，赛西可能需要提前较短时间通知获证组织或不通知获证组织就对其进行审核。

3.7 审核报告

3.7.1 审核报告按不同阶段、不同内容分为审核组末次会议的“口头报告”、现场出具的“不符合项报告”、最终的书面“审核报告”。离开现场之前，审核组在末次会上以口头方式做出关于受审核方的管理体系是否符合认证标准要求的说明，并使受审核方有机会对审核发现及其依据提出质疑，并将审核中所发现的不符以不符合项的形式提供给受审核方，明确纠正及纠正措施要求。

3.7.2 审核组长完成不符合项验证后提交书面审核报告，经赛西认证批准后发给受审核方。

3.7.3 审核报告至少应包括或引用以下内容：

1） 认证机构名称；
2） 受审核方的名称和地址及其代表；
3） 审核类型（如初次认证、监督、再认证或其他类型）；
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，重点反映受审核方模型风险识别与控制情况、内部审核和管理评审的过程、所取得的模型绩效，受审核方实际情况与其预期安全目标之间存在的差距和改进机会；
13） 与合规相关的行政处罚和受审核方发生的突发事件，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受审核方大语言模型供应链安全管理体系的重要变更（适用时）；

15) 获证组织对认证证书和认证标志使用的控制情况（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申请的认证范围适宜性的结论。

3.8 不符合纠正及验证

针对审核过程中发现的问题，审核组开具不符合项或观察项，要求受审核方对每一不符合项或观察项加以确认，并告知受审核方完成纠正及纠正措施的日期及跟踪验证的方式。纠正措施的验证有书面验证，现场跟踪验证二种方式。由审核组根据受审核方不符合项的性质和纠正措施的要求确定其中一种有效的验证方式。

不符合整改时限如下：

a. 初次认证审核：一般不符合在 1 个月内完成，严重不符合在 6 个月内完成；

b. 监督审核：一般不符合在 1 个月内完成，严重不符合在 3 个月内完成；

c. 再认证审核：一般不符合在 1 个月内完成，严重不符合在原证书到期前完成。

审核组长负责审查受审核方提交的不符合项的纠正和纠正措施，验证有效性，将验证结果告知受审核方。

如果受审核方未能在规定时间内完成不符合的纠正和纠正措施，则不推荐受审核方通过认证/再认证或暂停其认证证书。

对于审核中发现的观察项，下一次审核的审核组负责评审观察项的整改情况。

3.9 认证决定

赛西认证在收到审核组提交的全套审核资料后，交赛西认证技术委员会进行审查（若存在不符合项，须由受审核方完成纠正措施并由审核组长验证合格），进入审批注册发证程序，技委会审查将在 15 个工作日内完成。

获准认证/注册的受审核方，应符合下列条件：

a. 与赛西认证签有正式管理体系认证合同，满足申请方条件；（见本文件第 2 章）

b. 认证审核程序符合规定要求，上报资料完整、手续齐全；

c. 文件化的大语言模型供应链安全管理体系符合认证标准或其他引用文件的要求；

d. 组织依照文件化的管理体系运行有效（特别要有充分的证据表明组织对管理评审和内部审核进行了安排和有效地实施，并得以保持），对赛西认证审核时提出的不符合项已按要求全部完成了纠正措施并经审核组验证符合要求。

受审核方不能满足上述要求或者存在以下情况的，评定该受审核方不符合认证要求，客户部以书面形式告知受审核方并说明其未通过认证的原因。

a. 受审核方的大语言模型供应链安全管理体系有重大缺陷，不符合认证依据标准的要求。

b. 发现受审核方存在与大语言模型供应链安全管理体系相关的严重违法违规行为。

审查结果符合申请大语言模型供应链安全管理体系标准要求的，赛西认证将向受审核方提供经批准的书面审核报告以及由赛西认证总经理签发的认证合格证书并进行注册登记，证书有效期为三年。

赛西认证在机构网站上发布赛西认证管理体系认证合格组织名录，用以向社会各界证实认证合格组织符合有关管理体系标准的要求，同时为用户与获证组织建立合同关系提供选择指南。

赛西认证利用各种机会向国内外用户介绍管理体系认证合格组织，并接受国内外用户对有关情况的查询。

3.10 证书有效期内的情况通报

获证组织发生以下情况时，需及时联系赛西认证（联系方式见附录 3），进行信息通报：

a. 客户及相关方有重大投诉；

b. 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；

c. 发生与管理体系相关的重大事故；

d. 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；联系方式变更；管理体系覆盖的活动范围变更；管理体系和重要过程的重大变更等。需特别关注，赛西认证将随时更新认证范围内的多场所清单。为确保该信息的准确性，客户组织应将认证所涵盖的任何场所的关闭情况通知赛西认证，未通知的情况将被视为误用认证；

e. 出现影响管理体系运行的其他重要情况（如管理体系标准变更或体系认证范围扩大或缩小等）等。

获证组织通报时需填写《管理体系信息通报表》（见附录 2），并附上必要的资料或说明。一般情况下，应在更改/变动后 1 个月内通知赛西认证客户服务部，如发生上述 b)、c)条情况时，应在事故或问题发生后 48 小时内通知赛西认证客户服务部（特殊情况不超过 1 周，以电话方式通报的，需补填《管理体系信息通报表》），赛西认证根据情况决定是否进行现场调查，或实施管理体系复审，复审不受正常监督审核频次的限制。赛西认证将根据复审结果，做出换发证书或认证撤销的决定。

3.11 认证要求的变更

当认证要求发生变化时，赛西认证将以书面或其他方式将其认证要求的任何变更通知获证组织，并对其是否符合新的要求予以验证。为确保实施这些要求，获证组织可能需要与赛西认证补充签署或修订认证合同。

4 认证标志和认证证书

4.1 认证标志

赛西认证的管理体系认证合格标志（以下简称认证标志）是经国家工商行政管理部门登记的受法律保护的标志，由赛西认证随同管理体系认证合格证书（以下简称认证证书）一起颁发给获证组织合法使用，未经赛西认证允许，获证组织不得将此标志转让给其他组织或个人使用。

赛西认证的大语言模型供应链安全管理体系认证标志如下所示：



获证组织使用认证标志应符合上述规定的图案，尺寸可根据赛西认证提供的图样按比例放大或缩小，颜色应使用基本颜色或单一黑色。

4.2 认证证书

赛西认证的管理体系认证合格证书由赛西认证依据在国家认监委（CNCA）备案的证书（见

附录 4）要求进行统一制作、发放。未经赛西认证授权，其他组织或个人不得自行翻印或仿制。

4.2.1 认证证书内容

认证证书内容包括：

a. 获准认证组织名称、地址、社会信用代码、邮政编码、证书注册号（适用时包括总证书号和子证书号）、证书 OID 编号等；

b. 依据的管理体系标准和 / 或其他规范性文件的编号与版次；

c. 认证证书的生效期和有效期（变更情况发生时增加换证日期）；

d. 体系覆盖的范围描述；

e. 赛西认证的名称、地址与标志；

f. 赛西认证盖章（英文证书由公司总经理签字）；

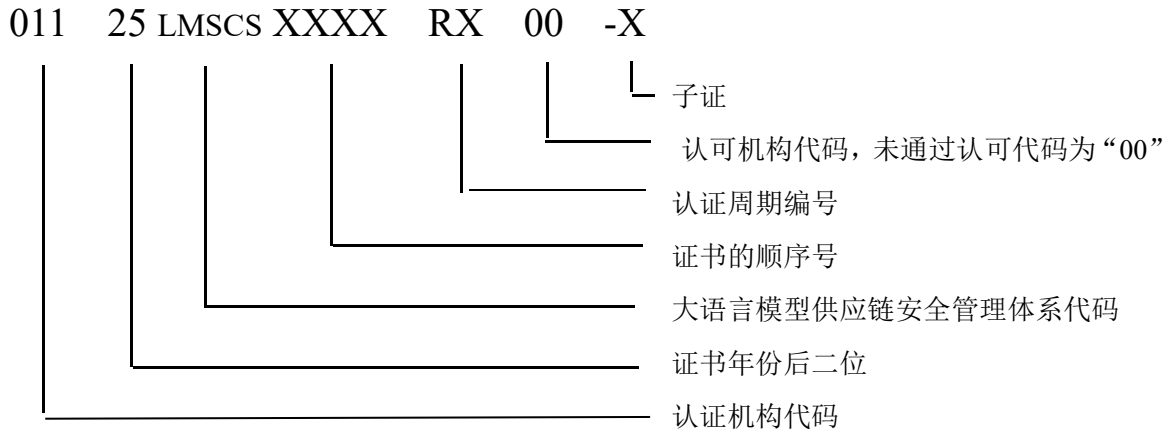
g. 适用时，相关的认可标识、认可注册号及国际互认标识；

h. 证书查询方式；

i. 认证证书相关附件（适用时）等。

4.2.2 证书编号

赛西认证大语言模型供应链安全管理体系获证组织认证证书编号规则如下：



认证周期编号，“R0”代表初次认证，R1 代表第一次再认证，R2 代表第二次再认证，以此类推。

4.3 认证标志和证书的使用

4.3.1 使用要求

4.3.1.1 认证证书和标志只证明获证组织的管理体系符合申请认证的管理体系标准的要求，不能证明获证组织生产的产品、活动符合其产品标准或产品安全认证标准的要求。获证组织可以将认证合格证书和标志作为符合管理标准要求的证明文件加以应用，但不得将该标志用在产品上，或作为产品的合格说明。获证组织不得将标志用于实验室检测、校准或检查的报告。

4.3.1.2 获证组织可以将证书和标志用在公开出版物、函件（包括信纸、信封）、传播媒介（如互联网、宣传册或广告）上，但不得引起产品（包括服务）或过程已通过认证的误解。若认证证书范围缩小，获证组织应随之修改所有相关的宣传资料。

4.3.1.3 获证组织可以在产品包装上或附带信息中声明其管理体系通过认证的管理规则。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。声明决不应暗示产品、过程或服务以这种方式得到了认证。声明应包含对下列的引用：

-- 获证组织的标识（例如品牌或名称）；

-- 管理体系的类型（例如质量、环境）和适用标准；

-- 本机构名称。

4.3.1.4 如果以某种方式明确说明了“生产该产品的管理体系通过了由赛西认证依据 GB/T 35770/ISO 37301 进行的认证”，则可将标志使用在运输产品的大箱子上（不能用在一个有形产品或在单个包装箱、容器等产品上，及在测试/分析活动中所出具的测试/分析报告）。

4.3.1.5 获证组织不得将认证标志使用在与认证范围无关的各类业务及其各类宣传载体上，进行误导宣传。

4.3.1.6 获证组织在使用认证标志时应接受赛西认证对认证证书和认证标志的正确使用的监督检查。

4.3.1.7 当获证组织的名称、地址或认证要求发生变化时，应提出申请换发认证证书，赛西认证将重新签发认证证书及附件。

4.3.2 使用申请

赛西认证客户服务部指定专人受理认证标志的使用申请。获证组织如需使用认证标志，

请与客户服务部联系，并说明使用的原因及方案。客户服务部经确认不违反标志的使用规定时，向获证组织提供电子版的认证标志。如存在问题，客户服务部应在收到申请后十五天内向申请组织提出。

4.4 违规处理

如发现获证组织对认证证书、标志的使用不符合要求、误用或有意错用认证标志、发生对赛西认证认证制度的不正确宣传时，赛西认证将根据其情节的轻重和引起不良影响后果，做出处理，包括：口头或书面警告、要求采取纠正或采取纠正措施、暂停证书、撤销证书资格和公告违规行为及必要的法律措施。

5 暂停、撤销、注销认证的条件及程序

5.1 暂停

5.1.1 获证组织有下列情况之一的，赛西认证在调查核实后的 5 个工作日暂停该组织的认证资格。

a. 因自身原因无法按时接受监督审核，超过规定期限的；

b. 大语言模型供应链安全管理体系持续地或严重地不满足认证要求及对管理体系有效性的要求，包括体系文件与实际业务运作严重脱离；

c. 不满足管理体系适用的法律法规要求，且未采取有效纠正措施的；

d. 拒绝配合认证监管部门实施的监督检查，或者提供虚假材料或信息的；

e. 错误使用认证证书、认证标志，未采取纠正措施的；

f. 被行政监管部门责令停业整顿的；

g. 被地方行政监管部门发现体系运行存在问题，需要暂停证书的；

h. 持有的与管理体系范围有关的行政许可文件、资质证书等过期失效的；

i. 受到与大语言模型供应链安全管理体系相关的行政处罚，且尚未完成整改的；

j. 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的；

k. 不承担、履行认证合同约定的责任和义务的；

l. 对于监督审核中提出的不符合项，未按规定时限进行纠正且无合理说明的（或纠正措施未被证实有效的）；

m. 发生管理体系相关重大事故，反映体系运行存在重大缺陷的；

n. 发生与大语言模型供应链安全管理体系相关重大舆情的；

o. 主动请求暂停的；

p. 其他应暂停认证证书的。

5.1.2 当做出证书暂停处理后，赛西认证将向获证组织发出“管理体系认证证书和标志变化通知”，通知获证组织其证书已被暂停。被暂停认证资格期间，获证组织不得以被认证的身份继续宣传其认证状态和使用认证标志。

5.1.3 一般情况下，认证资格暂停时间不超过 6 个月。

5.1.4 当被暂停认证资格的获证组织在赛西认证规定的期限内采取整改措施，并经验证满足规定的条件后，赛西认证将取消暂停，恢复其认证资格；超过规定时间后将撤销其认证资格，收回证书。暂停期间，经获证组织确认并同意后，可能在暂停期到期前撤销其认证资格。

5.2 撤销

5.2.1 获证组织有下列情况之一的，赛西认证在获得相关信息并调查核实后的 5 个工作日撤销其认证资格。

a. 被注销或撤销法律地位证明文件的；

b. 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；

c. 被暂停认证资格后，未在暂停期限内就存在问题采取相应有效的整改措施的；

d. 大语言模型供应链安全管理体系存在严重违反法律法规要求的；

e. 发生管理体系相关重大事故，经行政监管部门确认是获证组织违规造成的；

f. 没有运行管理体系或者因解散、破产、倒闭、经营不善或其它原因已不具备运行条件的；

g. 在认证有效期内，由于体系认证规则发生变更，获证组织不愿符合新要求的；

h. 严重违反与赛西认证正式协议中的有关规定，已造成了严重影响和后果且经查属实的；

i. 其他应撤销认证证书的。

5.2.2 当作出撤销获证组织的认证资格后，赛西认证向获证组织发出“管理体系认证证书和标志变化通知”，通知获证组织其证书已被撤销。被撤销认证资格的获证组织不得继续其所有利用认证资格的活动，并按赛西认证的要求交回认证证书。

5.3 注销

5.3.1 获证组织主动申请不再保持认证证书时，赛西将在确认其不存在暂停或撤销情形后，注销其认证证书。

5.3.2 当作出注销获证组织的认证资格后，赛西认证向获证组织发出“管理体系认证证书和标志变化通知”，通知获证组织其证书已被注销。被注销认证资格的获证组织不得继续其所有利用认证资格的活动，并按赛西认证的要求交回认证证书。

5.4 公示

获证组织的认证证书被暂停、撤销或注销后，赛西认证将在官方网站上进行公示，并按要求上报国家认监委（CNCA）。

6 申诉、投诉

6.1 管理体系认证的申请方、受审核方以及其他组织和个人均可对赛西认证与认证有关的工作提出申诉或投诉。

6.2 申、投诉的详细规定见赛西认证公开文件《申诉、投诉和争议处理规则》。

7 收费

7.1 赛西认证是经中国合格评定国家认可委员会（CNAS）认可的，不以营利为目的的，自负盈亏、独立核算的第三方管理体系认证机构，其认证业务活动费用来自认证收费。

7.2 收费项目包括：

a.固定费用，含：1）申请费

2）注册费

3）证书费

4）年金（如标志使用费、管理费）

b.认证审核费，含： 1）文件审查费

2）现场审核费

c.交通、食、宿费（由受审核方承担或据实收取）

d.监督审核费：包括现场审核费和年金，在证书有效期内按照合同约定的周期实施监督

审核，最后一次监督审核将同证书三年有效期满的再认证一起进行。

固定费用收费见赛西认证公开文件《管理体系认证/注册收费标准》

审核费根据受审核方的规模大小，审核现场场地分布，产品复杂程度以及申请的认证用标准，所需人日数来核定审核费。

8 其他

本认证规则由北京赛西认证有限责任公司批准后实施。

附录 1 国家认证认可监督管理委员会批文

附录 2 管理体系信息通报表

附录 3 CESI 认证业务联系方式

附录 4 认证证书样式

附录 5 审核时间

附录 1 国家认证认可监督管理委员会批文



认证机构批准书

批　　准　　号：CNCA-R-2002-011
机　构　名　称：北京赛西认证有限责任公司
住　　所：北京市东城区安定门东大街一号院1号楼2层
法定代表人：段淼
注　册　资　本：1000 万元
统一社会信用代码：9111010156749550XW
法　人　类　型：股份有限公司

认证业务范围：见附页
颁　发　日　期：2002年12月10日
换　发　日　期：2025年01月02日
有　效　期　至：2030年12月10日

国家认证认可监督管理委员会

附录 2　管理体系信息通报表

组织名称			
通讯地址			
采用标准	□GB/T 19001-_____　□GB/T 24001-_____　□GB/T 45001-_____ □GB/T 22080-_____　□ISO/IEC 20000-1：_____□GB/T 23331-_____ □GB/T 30146_____　□其他：_____		
注册号		证书有效期	
联系人		电　话	
邮　箱			
认证范围			

一、本组织管理体系的更改（在相应说明□中打 √，并随附相应更改的信息）。

1. 获证组织名称变更（提供变更后的营业执照）　□
2. 获证组织法定代表人、最高管理者变更（提供变更后的营业执照）　□
3. 获证组织法律地位 、生产经营状况、组织状态或所有权变（提供变更后的营业执照）□
4. 联系人信息变更（注明联系人名称、职务、手机、座机、邮编、传真）　□
5. 地址变更（注册地址、通讯地址、审核覆盖地址的变更）（注册地址变更提供变更后的营业执照；审核覆盖地址变更提供管理手册）　□
6. 行政许可资格、强制性认证或其他资质证书变更（提供变更后的资质许可证书）　□
7. 专业范围或生产制造或产品/活动范围变更（如需变更认证范围，需提交申请表，营业执照）　□
8. 能源管理体系的边界变更(EnMS 适用）（提供变更后的边界文件）　□
9. 违法法律法规的情况　□
10. 管理体系和重要过程的重大变更　□
11. 体系内人数变更　□
12. 其他方面变更　□

变更详细描述（可另附相关资料）	变更内容详述： 变更时间节点：□结合监督变更 □单独变更

二、企业发生事故（产品质量、职业健康安全、环境、信息安全、IT 服务、能源事故、业务连续性事故等）：

三、执法部门检查时发现的问题或重大投诉情况（请写明时间、地点、经过、原因分析、结果）：

签发人（单位盖章）：　　年　月　日

备注：如以上变更涉及到审核人日增加的，审核费用按实际增加人日收取。涉及证书更换的，另需交纳换发证书费（500 元/套）。如需增加证书副本，100 元/套。

附录 3　CESI 认证业务联系方式

部门	工作内容	联系电话
客户服务部	● 认证申请受理、合同洽谈； ● 认证后服务、认证交费、证书制作、证书领取； ● 申、投诉受理； ● 认证证书、标志使用申请受理 ● 体系变更通报受理	010-64102688 010-64102689 010-64102698
审查一部、审查二部、技术研发部/绿色低碳部	● 审核计划安排； ● 认证证书、标志使用的监督管理 ● 新业务领域的技术储备； ● 认证技术支撑	010-64102706 010-64102685 010-64102682
技术委员会	● 认证评定	010-64102691

附录 4　认证证书样式



管理体系认证证书

证书编号：0112XLMSCSXXXRX00
OID 编号：1.2.156.1.2.0112XSCS1XXXXRXX

兹证明

XXXXXXXXXXXX

（统一社会信用代码：XXXXXXXXXXXXXXXXX）
（XX 市 XX 区 XX 路 XX 号，XXXXXX）

大语言模型供应链安全管理体系符合标准：

WDTA AI-STR-03 《大语言模型供应链安全要求》

本证书覆盖下述范围：

XXXXXXXXXXXXXX

该认证范围覆盖场所：

XX 市 XX 区 XX 路 XX 号

本证书有效性依据发证机构的定期监督获得保持。证书有效性信息请登录 www.cc.cesi.cn 进行查询
（注：认证注册范围不包括未获得有效的国家规定的相关行政许可（含资质许可）的产品服务范围）

签发人：

发证机构：北京赛西认证有限责任公司

发证日期：20xx 年 xx 月 xx 日
换证日期：20xx 年 xx 月 xx 日
有效期至：20xx 年 xx 月 xx 日

地　　址：北京市东城区安定门东大街一号院 1 号楼 2 层
客服电话：4000719000　　网址：www.cc.cesi.cn



CERTIFICATE OF MANAGEMENT SYSTEM CERTIFICATION

ertificate No：0112XLMSCSXXXRX00
OID No：1.2.156.1.2. 0112X SCS1XXXXRXX

This is to certify that the This is to certify that the Large Language Model Security Requirements for Supply Chain Systems of

XXXXXXXXXXXXXXX
(Unified Social Credit Code: XXXXXXXXXXXXXXXXXX)
(xxxxxxxxxxxxxx,x, xxxxxxxx)

has complied with the requirements of

WDTA AI-STR-03

Large Language Model Security Requirements for Supply Chain

This certificate is valid for the following scope:

XXXXXXXXXXXXXXX

The Location Covered By The Certification Is:

xxxxxxxxxxxxxxxxxxxx

THE VALIDITY OF THIS CERTIFICATE DEPENDS ON THE CONSEQUENCE OF THE ANNUALLY SURVEILLANCE EXECUTED BY THE CERTIFICATION BODY
PLEASE ACCESS www.cc.cesi.cn FOR CHECKING VALIDITY OF THE CERTIFICATE
Note: The scope of product services without the related administrative permits and qualifications is not included in the scope of certification registration.

SIGNATURE:　　CESI Certification Co., Ltd.

Issue Date:20xx-xx-xx
Exchange Date: 20xx-xx-xx
Valid Until: 20xx-xx-xx

Add: 2nd Floor, Building 1, No.1 Andingmen Dongdajie, Dongcheng District, Beijing,China
Tel:4000719000　　http://www.cc.cesi.cn

附录 5 审核时间

大语言模型供应链安全管理体系审核时间要求

员工人数	参考人日数		
	初次认证	监督审核	再认证
1	1.5	1	1
2～10	3	1	2
11～30	6	2	4
31～100	8	3	5.5
101～500	12	4	8
501～2000	15	5	10
＞2000	延用以上规律		

注:

1. 有效人数包括认证范围内涉及的所有人员(含每个班次的人员)。认证范围内覆盖的非固定人员(如承包商人员)和兼职人员也应包括在有效人数内。

2. 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确定，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。

3. 认证委托人正常工作期间(包括轮班)安排的审核时间可以计入有效的管理体系认证审核时间，但往返多个审核场所之间所花费的路途时间不计入有效的管理体系认证审核时间。

4. 增减审核时间所考虑的因素按机构相关作业指导书执行。