文件编号：XR-GZ-2025-55

鑫锐认证有限公司

编制日期：2025 年 6 月 10 日

实施日期：2025 年 6 月 23 日

文件编号：XR-GZ-2025-55

数据治理安全管理体系认证实施规则

编制日期：2025 年 6 月 10 日

实施日期：2025 年 6 月 23 日

目录

1 适用范围

1.1 本规则用于规范鑫锐认证有限公司(以下简称“本机构”)依据相关标准在中国境内开展的数据治理安全管理体系认证活动。

1.2 本规则依据认证认可相关法律法规，结合相关技术标准，对数据治理安全管理体系认证实施过程作出具体规定，明确本机构对认证过程的管理责任，保证数据治理安全管理体系认证活动的规范、有效。

1.3 本规则是本机构在数据治理安全管理体系认证活动中的基本要求，所有认证人员在该项认证活动中应遵守本规则。

1.4 本规则覆盖可颁发的证书包括：数据治理安全管理体系认证证书。

2 认证依据

GB/T 27021.1《合格评定管理体系审核认证机构要求》

ISO/IEC 38505-1:2017《信息技术-信息技术的治理-数据的治理》

3 对认证人员的基本要求

3.1 审核人员应具有 CCAA 注册的管理体系认证审核员&服务审查员资格。

3.2 认证人员应经过 ISO/IEC 38505-1:2017《信息技术-信息技术的治理-数据的治理》的培训；审核人员应经评价具备数据治理安全管理体系认证体系的能力。

3.3 认证人员应当遵守与从业相关的法律法规，对认证活动及相关认证记录、认证审核报告的真实性承担相应的法律责任。

4 初次认证程序

4.1 受理认证申请

4.1.1 申请认证的组织可从本机构网站直接获取或通过适当途径获取以下信息：

a)可开展认证业务的范围，以及获得认可的情况；

b)本规则的完整内容；

c)认证证书样式；

d)对认证过程的申诉、投诉规定；

e)申请书、认证合同等格式文件。

4.1.2 申请书及申请组织至少提交以下资料：

由认证申请方填写《认证申请书》，并按其附件要求提供申请认证所需资料。资料包括，但不限于：

a)有效的营业执照复印件；

b)现行有效的数据治理安全管理体系认证体系文件及文件清单；

c)涉及国家法规强制要求的有效许可文件，如：服务/卫生/经营许可证等；

d)与经营过程有关的法律、法规及标准、技术规范（国际、国家、地方、行业）的清单（可放入数据治理安全管理体系认证体系文件中，如管理手册；）

e)组织机构图（可放入数据治理安全管理体系认证体系文件中，如管理手册；）

f)主要的经营过程描述（可放入数据治理安全管理体系认证体系文件，如管理手册中。）

4.2 申请评审

4.2.1 评审要求

4.2.1.1 本机构对申请组织提交的申请资料进行评审，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。

4.2.1.2 申请组织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，本机构将不受理其认证申请；

4.2.1.3 申请组织若涉及环境影响评价、排污许可等完整环保手续，需提供相关资料并且需满足近三年无重大环境违法违规记录。

4.2.1.4 评审内容包括，但不限于：

a)申请组织基本信息及其服务相关信息的充分性，了解组织特点，确定申请组织法律地位的合法性，必要时，通过公开网站验证提供信息的真实性、有效性；

b)申请组织对于认证要求的信息是否已全部获知，并愿意遵守；对于认证要求的信息理解上的差异是否已得到解决。初步确定可受理的认证范围；

c)本机构的专业能力是否满足审核实施的要求 ,包括认证审核人员和认证决定人员的能力是否满足要求。

对评审后确定无法受理的认证项目，本机构将在 5 日内通知认证申请方。对不予受理的申请或申请方撤回的申请，应采取保密方式将申请文件和有关的资料归档保存。

4.2.2 签订认证合同

受理申请后，本机构将与申请组织订立具有法律效力的书面认证合同，合同包含以下内容：

a)申请组织获得认证后持续有效运行管理体系并保持标准化控制水平的承诺。

b)申请组织对遵守认证认可相关法律法规，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的承诺。

c)申请组织承诺获得认证后发生以下情况时，应及时向本机构通报：

①客户及相关方有重大投诉。

②提供的产品或服务被市场监管部门认定不合格。

③发生了与其产品或服务相关的重大事故。

④管理体系和重要过程的重大变更，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；法定代表人、最高管理者变更；经营场所变更；管理体系覆盖的活动范围变更等。

⑤出现影响管理体系运行的其他重要情况。

d)申请组织承诺获得认证后正确使用认证证书、认证标志和有关信息。

e)拟开展的数据治理安全管理体系认证覆盖的范围。

f)在认证审核实施过程及认证证书有效期内，本机构和申请组织各自应当承担的责任、权利和义务。

g)认证服务的费用（费用计算方法见公司相关文件）、付费方式及违约条款。

4.2.3 认证信息或认证要求变更申请的评审

获证组织提出组织名称、地址、认证范围的变更或认证要求的变更申请时，需填报《获证组织认证信息确认表》，并提交必要的补充信息。本机构将对变更内容进行评审，且要特别关注其申请变更资料的充分性和合法性。经评审确认不能受理的，将及时反馈申请组织说明理由。

4.3 审核策划

4.3.1 制定审核方案

4.3.1.1 依据本机构相关文件要求，综合考虑组织的规模、行业特点、运作的复杂程度、经营场所的数量，以及经过证实的数据治理安全管理体系认证体系管理体系有效性水平和以前审核结果，制定整个认证周期的审核方案，并通过每次审核结束后的反馈信息和审核前再次获取的变化信息，包括及时作出原有审核方案的调整，以实现动态的管理。

4.3.1.2 为确保认证审核的完整有效，本机构将基于申请组织管理体系覆盖的有效人数，并考虑服务活动范围、特性、技术复杂程度、风险程度等情况，核算并拟定完成认证审核工作需要的现场审核人日数。在特殊情况下，可以减少审核时间，但减少的时间不得超过附录 B 所规定的审核时间的 30%。

4.3.1.3 整个审核时间中，现场审核时间不应少于总审核时间的 80%。

4.3.2 组成审核组

4.3.2.1 本机构将根据管理体系覆盖的活动选择具备相关能力的审核员组成审核组，必要时可以选择技

术专家参加审核组。

4.3.2.2 技术专家主要负责提供认证审核的技术支持，不作为审核员实施审核，不计入审核时间，其在审核过程中的活动，由审核组中的审核员承担责任。

4.3.3 审核通知

确定审核时间和审核组后，拟定审核通知，发给受审核方，经受审核方确认后，发给审核组。

4.3.4 审核计划

4.3.4.1 审核组接到审核通知书后，制定书面的审核计划（包括多场所抽样计划），以便为有关各方就审核活动的安排和实施达成一致提供依据。

4.3.4.2 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。

4.3.4.3 为使现场审核活动能够观察到服务活动情况，现场审核应安排在认证范围覆盖的服务活动正常运行时进行。

4.3.4.4 在审核活动开始前，审核组应将审核计划交申请组织确认，遇特殊情况临时变更计划时，应及时将变更情况通知申请组织，并协商一致。

4.4 实施审核

4.4.1 总要求

数据治理安全管理体系认证审核分为初审（文件评审+现场审核）、监督审核（第一次、第二次）、再认证审核类型，审核组将按照审核计划的安排完成审核工作。现场审核中的“现场”指认证范围内的各类活动完成的主要场所，一般情况下，是组织人员集中的地方。

4.4.2 文件审核

文件审核将在现场审核之前完成（不占审核人日）。依据相应标准及相关法律法规要求对申请组织的管理体系文件进行符合性、适宜性和充分性的审核，当审核过程中发现文件存在不符合而影响管理体系的

运行时，应告知申请组织进行及时的纠正和纠正措施，以确保管理体系控制水平达到标准要求。必要时，可在现场审核前实施文件审核，根据文件审核结果确定是否或何时安排现场审核。

4.4.3 首末次会议

审核组应当会同受审核方按照程序顺序召开首、末次会议，受审核方的最高管理者及与管理体系相关的职能部门负责人员应参加会议。参会人员应签到，审核组应当保留首、末次会议签到表。受审核方要求时，审核组成员应向申请组织出示身份证明文件。

4.4.4 审核方法

4.4.4.1 现场审核审核方式包括：

a)交谈；

b)查阅资料；

c)现场观察；

d)可行时，现场测试或测量。

4.4.4.2 审核组依据相应标准要求进行审核。

4.4.5 编制审核报告。

4.4.5.1 每次审核结束后，审核组长应依据现场审核中发现的相关信息，编制《审核报告》，并对报告的内容负责，经技术委员会批准后发放到认证申请方。

4.4.5.2 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，并应包括如下内容：

a)客户的名称和地址及其管理者代表；

b)审核类型（如初次认证、监督或再认证审核）

c)审核的目的、范围和准则；

d)审核组成员及审核时间；

e)与有关认证要求符合性的陈述；

f)报告覆盖的时间段；

g)不符合项的情况；

h)审核结论。

4.5 不符合项的纠正和纠正措施及其结果的验证

4.5.1 对审核中发现的不符合项，本机构应要求申请组织分析原因，并要求申请组织在规定期限内采取措施进行纠正。

4.5.2 本机构应对申请组织所采取的纠正和纠正措施及其结果的有效性进行验证。

4.6 认证决定

4.6.1 本机构应该在对审核报告、不符合项的纠正和纠正措施及其结果进行综合评价基础上，作出认证决定。

4.6.2 审核组成员不得参与对审核项目的认证决定。

4.6.3 本机构在作出认证决定前应确认如下情形：

a)审核报告符合本规则第 4.4 条要求，能够满足作出认证决定所需要的信息。

b)反映以下问题的不符合项，本机构已评审、接受并验证了纠正和纠正措施及其结果的有效性。

①未能满足数据治理安全管理体系认证体系标准的要求。

②制定的管理目标不可测量、或测量方法不明确。

③对实现管理目标具有重要影响的关键点的监视和测量未有效运行，或者对这些关键点的报告或评审记录不完整或无效。

④在持续改进数据治理安全管理体系认证体系的有效性方面存在缺陷，实现管理目标有重大疑问。

c)本机构对其他不符合项已评审，并接受了申请组织计划采取的纠正和纠正措施。

4.6.4 在满足 4.6.3 条要求的基础上，本机构有充分的客观证据证明申请组织满足下列要求的，评定该

申请组织符合认证要求，向其颁发认证证书。

a)申请组织的数据治理安全管理体系认证体系符合标准要求且运行有效。

b)认证范围覆盖的产品或服务符合相关法律法规要求。

c)申请组织按照认证合同规定履行了相关义务。

4.6.5 申请组织不能满足上述要求的，评定该申请组织不符合认证要求，以书面形式告知申请组织并说明其未通过认证的原因。

4.6.6 本机构在颁发认证证书后，应当在 30 个工作日内按照规定的要求将相关信息报送国家认监委。国家认监委在其网站（www.cnca.gov.cn）开设专栏向社会公开本机构上报的认证证书信息。

4.6.7 本机构不得将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。

5 监督审核程序

5.1 本机构应对持有其颁发的数据治理安全管理体系认证证书的组织(以下称获证组织)进行有效跟踪，监督获证组织通过认证的数据治理安全管理体系认证体系持续符合要求。

5.2 为确保达到 5.1 条要求，本机构应根据获证组织的食品配送安全风险程度或其他特性，确定对获证组织的监督审核的频次。

5.2.1 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。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。

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。

5.2.2 在达到第二次监督审核期限而有证据表明获证组织暂不具备实施监督审核的条件时，可以适当延长监督审核期限，但最长间隔不能超过 15 个月。

5.2.3 超过期限而未能实施监督审核的，应按 7.2 或 7.3 条处理。

5.3 监督审核的时间，按公司相关文件计算。

5.4 监督审核的审核组，应符合 4.3.2 条的要求。

5.5 监督审核可采用在获证组织现场或非现场的方式进行。由于产品生产的季节性原因，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。

5.6 监督审核时至少应审核以下内容：

a)上次审核以来数据治理安全管理体系认证体系覆盖的活动及运行体系的资源是否有变更。

b)重要关键点是否按数据治理安全管理体系认证体系的要求在正常和有效运行。

c)对上次审核中确定的不符合项采取的纠正和纠正措施是否继续有效。

d)数据治理安全管理体系认证体系覆盖的活动涉及法律法规规定的，是否持续符合相关规定。

e)管理目标是否实现。适用时，目标没有实现的，获证组织在内部管理评审时是否及时调查、分析原因并采取了改进措施。

f)获证组织对认证标志的使用或对认证资格的引用是否符合相关的规定。

g)适用时，内部审核和管理评审是否规范和有效。

h)是否及时接受和处理投诉。

i)适用时，针对内审发现的问题或投诉的问题，及时制定并实施了有效的持续改进。

5.7 监督审核的审核报告，应按 5.6 条列明的审核要求逐项描述审核证据、审核发现和审核结论。审核组应提出是否继续保持认证证书的意见建议。

5.8 本机构根据监督审核报告及其他相关信息，作出继续保持或暂停、撤销认证证书的决定。

6 再认证程序

6.1 认证证书期满前，若获证组织申请继续持有认证证书，本机构应当实施再认证审核决定是否延续认证证书。

6.2 本机构应按 4.3.2 条要求组成审核组。按照 4.3 条要求并结合历次监督审核情况，制定再认证计划并交审核组实施。审核组按照要求开展再认证审核。在数据治理安全管理体系认证体系及获证组织的内部和外部环境无重大变更时，按公司相关文件确定再认证的审核时间。

6.3 对再认证审核中发现的不符合项，应按 4.5 条要求实施纠正和纠正措施并进行验证，验证应在原证书有效期满前完成。

6.4 本机构参照 4.6 条要求作出再认证决定。获证组织继续满足认证要求并履行认证合同义务的，向其换发认证证书。

7 暂停或撤销认证证书

7.1 本机构应制定暂停、撤销认证证书或缩小认证范围的规定，并形成文件化的管理制度。

7.2 暂停证书

7.2.1 获证组织有以下情形之一的，本机构应在调查核实后的 5 个工作日内暂停其认证证书。

a)数据治理安全管理体系认证体系持续或严重不满足认证要求 ,包括对数据治理安全管理体系认证体系运行有效性要求的。

b)不承担、履行认证合同约定的责任和义务的。

c)被有关执法监管部门责令停业整顿的。

d)被地方认证监管部门发现体系运行存在问题，需要暂停证书的。

e)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的。

f)主动请求暂停的。

g)其他应当暂停认证证书的。

7.2.2 认证证书暂停期不得超过 6 个月。但属于 7.2.1 第 e 项情形的暂停期可至相关单位作出许可决定

之日。

7.2.3 本机构暂停认证证书的信息，应明确暂停的起始日期和暂停期限，并声明在暂停期间获证组织不得以任何方式使用认证证书、认证标识或引用认证信息。

7.3 撤销证书

7.3.1 获证组织有以下情形之一的，本机构应在获得相关信息并调查核实后 5 个工作日内撤销其认证证书。

a)被注销或撤销法律地位证明文件的。

b)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和调查提供了虚假材料或信息的。

c)出现重大的食品配送安全责任事件，经执法监管部门确认是获证组织违规造成的。

d)有其他严重违反法律法规行为的。

e)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的（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）。

f)没有运行数据治理安全管理体系认证体系或者已不具备运行条件的。

g)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 6 个月仍未纠正的。

h)其他应当撤销认证证书的。

7.3.2 撤销认证证书后，本机构应及时收回撤销的认证证书。若无法收回，本机构应及时在相关媒体和网站上公布或声明撤销决定。

7.4 本机构暂停或撤销认证证书应当在其网站上公布相关信息，同时按规定程序和要求报国家认监委。

7.5 本机构有义务和责任采取有效措施避免各类无效的认证证书和认证标志被继续使用。

8 认证证书要求

8.1 认证证书应至少包含以下信息：

a)获证组织名称、地址和组织机构代码。该信息应与其法律地位证明文件的信息一致。

b)数据治理安全管理体系认证体系覆盖的生产经营或服务的业务范围。若认证的数据治理安全管理体系认证体系覆盖多场所，表述覆盖的相关场所的名称和地址信息，该信息应与相应的法律地位证明文件信息一致。

c)数据治理安全管理体系认证体系符合标准的表述。

d)证书编号。

e)本机构名称。

f)证书签发日期及有效期的起止年月日。对初次认证以来未中断过的再认证证书，可表述该获证组织初次获得认证证书的年月日。

g)证书查询方式。本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。

8.2 认证证书有效期为 3 年。

8.3 本机构应当建立证书信息披露制度。除向申请组织、认证监管部门等执法监管部门提供认证证书信息外，还应当根据社会相关方的请求向其提供证书信息，接受社会监督。

9 与其他服务、管理体系的结合审核

9.1 对数据治理安全管理体系认证体系和其他管理体系实施结合审核时，通用或共性要求应满足本规则要求，审核报告中应清晰地体现 4.4 条要求，并易于识别。

9.2 结合审核时，应按公司审核时间确定规范核算结合审核的审核人日数。

10 受理转换认证证书

10.1 本机构应当履行社会责任，严禁以牟利为目的受理不符合 ISO/IEC 38505-1:2017《信息技术-信息技术的治理-数据的治理》、不能有效执行数据治理安全管理体系认证体系的组织申请认证证书的转换。

10.2 本机构受理组织申请转换本机构的认证证书，应该详细了解申请转换的原因，进行必要的现场审核。

10.3 转换仅限于现行有效认证证书。被暂停或正在接受暂停、撤销处理的认证证书以及已失效的认证证书，不得接受转换申请。

10.4 被执法监管部门责令停业整顿或列入“黑名单”的（如 7.2 条第 c 项）、被发证机构撤销证书的（如 7.3 条），除非该组织进行彻底整改，导致暂停或撤销认证证书的情形已消除，否则不应受理其认证申请。

11 受理组织的申诉

获证组织对认证决定有异议时，本机构应接受获证组织申诉并且及时进行处理，在 60 日内将处理结果形成书面通知送交获证组织。

书面通知应当告知获证组织，若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，可以直接向所在地认证监管部门或国家认监委投诉。

12 认证记录的管理

12.1 本机构应当建立认证记录保持制度，记录认证活动全过程并妥善保存。

12.2 记录应当真实准确以证实认证活动得到有效实施。记录资料应当使用中文，保存时间至少应当与认证证书有效期一致。

12.3 以电子文档方式保存记录的，应采用不可编辑的电子文档格式。

13 收费

数据治理安全管理体系认证收费参考本机构的管理体系认证收费标准收取。

14 其他

14.1 本规则内容提及 ISO/IEC 38505-1:2017《信息技术-信息技术的治理-数据的治理》标准时均指认证活动发生时该标准的有效版本。认证活动及认证证书中描述该标准号时，应采用当时有效版本的完整标准号。

14.2 本规则所提及的各类证明文件的复印件应是在原件上复印的，并经复印件提供者签章（签字）认可其与原件一致。

14.3 本机构可采取必要措施帮助组织开展数据治理安全管理体系认证体系及相关技术标准的宣贯培训，促使组织的全体员工正确理解和执行数据治理安全管理体系认证体系标准。

附录 A：

数据治理安全管理体系认证体系审核时间要求

有效人数	审核时间（人天）
1-200	1
201-500	2
>501	3

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)。覆盖于认证范围内的非固定人员(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。

3.组织正常工作期间(如轮班制组织)安排的审核时间可以计入有效的体系认证审核时间，但往返多审核场所之间所花费的时间不计入有效的管理体系认证审核时间。

4.涉及多个固定场所或临时场所，需根据场所数量、路程，每个场所增加 0.5-1 人天。