BSC-03-W-01-DSMM-2025

版号： B/0

数据安全能力成熟度管理体系认证规则

编制：丁　睿　2026.03.02

审核：张　敬　2026.03.02

批准：孙竹君　2026.03.02

三星九千认证
Beijing Sanxing 9000 Certification Body Co.,Ltd.

目　录

1. 适用范围

1.1. 本规则适用于北京三星九千认证中心公司有限公司（以下简称“公司”）对申请组织按照GB/T 22080-2025/ISO 27001:2022 《网络安全技术 信息安全管理体系 要求》及GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》，从组织建设、制度流程、技术工具和人员能力等四个方面，建立的数据安全能力的成熟度（简称DSMM）开展认证活动。

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，对数据安全能力成熟度模型认证实施过程作出具体规定，是公司从事数据安全能力成熟度模型认证活动的基本依据，保证数据安全能力成熟度模型认证活动的规范有效。

1.3. 本规则是对数据安全能力成熟度模型认证活动的基本要求，公司在该项认证活动中应当遵守本规则。除本文件规定的特定要求外，应遵循公司基本管理要求和各项管理制度。

2. 认证依据

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

GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型

3. 初次认证程序

3.1. 认证申请

3.1.1. 申请人应具备以下条件：

（1）具有法律地位或授权，承诺遵守适用法律法规的要求；

（2）已取得相关法规规定的行政许可文件，并在有效期内；

（3）已按照 GB/T 22080-2025/ISO 27001:2022、GB/T 37988标准及相应行业认证要求建立了DSMM 且体系正常运行三个月以上；

（4）遵守有关主管部门对数据安全相关的强制性要求，或相关要求（适用时）；

（5）近三年内无违法、违规、失信记录。

3.1.2. 申请组织至少应提交的文件和资料:

（1） 认证申请书（申请认证的范围、成熟度等级或其他要求）；

（2） 申请组织的一般特征，包括其名称、物理场所的地址、过程和运营的核心业务以及任何相关的法律义务；

（3） 组织机构图（含有效人数）；

（4） 营业执照和有效期内的涉及国家法规强制要求的许可文件；

（5） 合同管理边界说明，涉及多个场所时，各场所的名称、地址及其管理内容；

（6） 现行有效的管理体系文件及文件清单；

（7） 其他所需文件。

3.2. 认证受理

3.2.1. 公司应向申请人至少公开认证工作程序、认证依据、认证流程、认证证书样式及认证标志及相关的使用规定等相关信息，同其他管理体系。

3.2.2. 申请评审

3.2.2.1. 公司应实施认证申请评审，根据公司能力确定是否受理认证申请。公司应根据认证依据、程序等要求，对申请人提交的申请文件和资料进行评审并保存评审记录，以确保：

（1） 认证要求规定明确、形成文件并得到理解；

（2） 公司和申请人之间在理解上的差异得到解决；

（3） 对于申请的认证范围、成熟度等级、风险等级、申请人的工作场所和任何特殊要求，公司均有能力开展认证服务。

3.2.2.2. 存在以下情况的组织，公司不得受理其认证申请：

（1） 组织存在不符合3.1.1情形的；

（2） 被执法监管部门责令停业整顿期间的；

（3） 被全国企业信用信息公示系统或者政府其他信用公示系统列入严重违法失信名单的；

（4） 其他被政府主管部门认定或被媒体曝光有不符合、违规违法失信行为，且尚在处理期间的。

3.2.3. 评审结果处理

（1） 申请材料齐全、符合要求的，予以受理认证申请。

（2） 未通过申请评审的，应书面通知认证申请人在规定时间内补充、完善，或不同意受理认证申请并明示理由。

（3） 公司应完整保存认证申请评审的工作记录。

3.2.4签订认证合同

在实施认证审核前，公司应与每个申请组织订立具有法律效力的认证合同或等效文件，以明确双方的责任，合同应至少包含的内容同其他管理体系。

3.3. 审核策划

3.3.1. 审核方案策划

3.3.1.1. 公司应针对每一认证客户建立认证周期内的审核方案，包括初次认证的审核方案、认证决定之后的变更审核和第三年在认证到期前进行的再认证审核。

3.3.1.2. 初次认证后的第一次监督审核应当在认证证书签发日起12个月内进行。此后，监督审核应当至少每个日历年（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12个月。

3.3.1.3. 公司应基于风险的方法进行审核方案策划，审核方案的确定和任何后续调整应考虑客户的规模、管理体系范围、复杂程度和风险大小，以及经过证实的管理体系有效性水平和以前审核的结果。

3.3.2. 审核时间

为确保认证审核的完整有效，公司应策划审核时间，根据申请组织数据安全能力成熟度模型覆盖的活动范围、特性、成熟度等级、技术复杂程度、风险程度、认证要求和体系覆盖范围内的有效人数等情况，核算并拟定完成审核工作需要的时间。在特殊情况下，可根据项目具体情况增加或减少评价时间时，理由应充分，并进行记录，可参考《数据安全能力成熟度认证管理方案》实施。

3.3.3. 审核组

3.3.3.1. 公司应当根据数据安全能力成熟度模型覆盖的活动选择具备相关能力的审核员组成审核组，审核组中的审核员承担审核任务和责任。

3.3.3.2. 通常情况下，审核组至少有一名具备国家注册正式信息安全管理体系审核员资格的人员。

3.3.3.3. 审核组的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。

3.3.4. 审核计划

公司应当为每次现场审核制定审核计划。审核计划要求执行公司《基本审核规范》要求。

3.4. 现场审核

审核组应当按照审核计划的安排完成审核工作，满足公司《审核基本规范》要求。对于数据安全能力成熟度模型审核的实施可参见《DSMM审核作业指导书》。

3.4.1. 第一阶段审核

3.4.1.1. 初次认证审核，可不进行一阶段现场审核，但应完成必要的文件审核。文件审核应依据公司文件评审相关要求对申请组织的数据安全能力成熟度模型文件进行适宜性和充分性的评审，当评审过程中发现文件存在不符合而影响数据安全能力成熟度模型的运行时，应告知申请组织进行及时的纠正和纠正措施。文件审核通过后，方可安排现场审核。

3.4.1.2. 一阶段主要审核内容，包括：

（1） 审核客户文件化的管理体系信息；

（2） 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；

（3） 审核客户数据安全能力成熟度模型的理解和实施标准要求的情况，特别是对数据安全能力成熟度模型的关键绩效或重大合规风险、合规义务、目标和运作的识别情况；

（4） 收集关于客户的管理体系范围的必要信息，包括：

——客户的场所；

——使用的信息系统和数据类型、数量；

——所建立的控制的水平（特别是客户为多场所时）；

——适用的法律法规要求。

（5） 审核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；

（6） 结合管理体系标准或其他规范性文件充分了解客户数据安全能力成熟度模型和现场运作，以便为策划第二阶段提供关注点；

（7） 评价客户是否策划和实施了自评估，以及数据安全能力成熟度模型的实施程度能否证明客户已为第二阶段做好准备。

3.4.2. 第二阶段审核

第二阶段审核应当依《认证机构远程审核指南》（T/CCAA 36-2022）的要求，决定是否需要现场进行，对照GB/T 22080-2025/ISO 27001:2022及GB/T 37988-2019标准全部条款评价申请组织数据安全管理的实施情况和体系的有效性，并至少覆盖以下方面：

（1） 与数据安全能力成熟度模型标准或其他规范性文件的所有要求的符合情况及证据；

（2） 依据关键绩效目标和指标（数据安全能力成熟度模型标准或其他规范性文件的期望一致）、成熟度等级，对绩效进行的监视、测量、报告和评审；

（3） 申请组织数据安全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） 申请组织的数据生命周期管控规程；

（5） 针对数据安全治理的管理职责。

3.5. 不符合纠正的验证

3.5.1. 审核组应当根据审核发现形成严重或轻微不符合，要求受审核方在规定的时限内对不符合进行原因分析、采取相应的纠正和纠正措施（轻微不符合可以是纠正措施计划）。公司应审查受审核方提交的纠正和纠正措施，以确定其是否可被接受。

3.5.2. 对于严重不符合（＜0.7分的过程域），要求受审核方在规定时间内完成整改；公司应当督促受审核方及时进行整改，并对其纠正和纠正措施的有效性进行验证。

3.5.3. 对于组织未能在规定的时限完成对不符合所采取措施的情况，审核组不应当给予该受审核方推荐认证、再认证、或推荐降级认证的决定。

3.6. 审核报告

3.6.1. 公司应当就每次审核向受审核方提供完整详实的审核报告。审核组长应对审核报告的内容负责。

3.6.2. 审核组应对审核活动形成书面审核报告，由审核组组长签字。审核报告的内容应当反映受审核方管理体系的真实状况，描述对照GB/T 22080-2025/ISO 27001:2022及GB/T GB/T 37988-2019标准，确定体系与标准条款的一致性及运行有效性的客观证据信息，及对认证结论的推荐意见。审核报告应准确、简明和清晰地描述审核活动的主要内容，包括内容按照其他管理体系，满足公司《审核基本规范》要求。

3.6.3. 公司应在作出认证决定后将审核报告提交申请组织，并保留用于证实审核报告中相关信息的证据。

3.6.4. 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，公司应将此报告及终止审核的原因提交给申请组织，并保留签收或提交的证据。

3.7. 复核和认证决定

3.7.1. 公司应根据审核过程中收集的信息和其他有关信息，对审核结果进行综合评价，特别是对组织的合规管理状况进行评价。必要时，公司应对申请人满足所有认证依据的情况进行风险评估，以做出申请组织所建立的数据安全能力成熟度模型能否获得认证的决定。

3.7.2. 公司应对审核报告、不符合项的纠正和纠正措施及其结果进行综合评价，并作出认证决定。认证决定人员应为公司管理控制下的人员，审核组成员不得参与对审核项目的认证决定。

3.7.3. 对于符合认证要求的申请人，认证机构应颁发认证证书。对于不符合认证要求的申请人，认证机构应以书面的形式明示其不能通过认证的原因。

3.7.4. 对认证决定的申诉

3.7.4.1. 申请人如对认证决定结果有异议，可在30个工作日内向公司申诉，公司自收到申诉之日起，应在一个月内进行处理，并将处理结果书面通知申请人。

3.7.4.2. 申请人如认为公司行为严重侵害了自身合法权益的，可以直接向认证监管部门投诉。

4. 变更审核程序

4.1 公司应对持有其颁发的该领域管理体系认证证书的组织（以下称获证组织）进行有效跟踪，监督获证组织持续运行并符合认证要求。

4.2 监督审核频次

认证机构应对获证组织制定针对性的监督审核方案，根据获证组织的管理体系成熟度确定监督

审核频次，但两次监督审核的时间间隔不应大于12个月。在获证组织核心领导层调整、数据治理架构变更、重大业务范围变更、信息系统变更、数据湖\数据仓\数据库变更、机房位置调整、数据安全事件整改后等重大变更后，应当及时增加监督审核频次，以保证监督审核的有效性。

4.3 监督审核的现场审核程序与初次认证现场审核程序基本相同。

4.4 监督不必覆盖客户管理体系的全部，但是应至少重点关注以下方面：

1）获证组织管理体系的预期目标的实现情况；

2）持续的运行控制和变化情况；

3）相关法律法规和行业要求变化情况及组织合规性评价的情况；

4）上次审核中确定的不符合采取的纠正措施的实施情况及有效性；

5）内部审核和管理评审；

6）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；

7）相关投诉的处理；

8）上次审核后发生的数据安全事故的调查与处理。

5. 再认证程序

5.1. 认证证书有效期满前三个月，获证组织可申请再认证。再认证程序与初次认证程序一致，公司应当实施再认证审核，并决定是否延续认证证书。

5.2. 在数据安全能力成熟度模型及获证组织的内部和外部环境无重大变更时，再认证审核时间应不少于初次认证审核人日数的2/3。

5.3. 再认证审核时至少应审核以下内容：

⑴ 结合内部和外部变更来看的整个数据安全能力成熟度模型的有效性，以及认证范围的持续相关性和适宜性；

⑵ 经证实的对保持数据安全能力成熟度模型有效性并持续改进，以提高整体绩效的承诺；

⑶ 数据安全能力成熟度模型在实现获证客户数据治理目标和预期结果方面的有效性。

6. 认证证书和认证标志的要求

6.1. 经认证决定，公司向符合要求的组织出具认证证书，认证证书的生效日期不早于认证决定的日期。数据安全能力成熟度认证证书有效期3年。

6.2. 认证证书载明的信息应全面、清晰、容易理解、设计上不会以任何方式产生误导。

6.3. 公司应按照《认证证书和认证标志管理办法》等相关要求对获证组织使用认证证书和认证标志的活动进行监督管理，并已在公司文件《获证须知》《认证资格及证后管理程序》中明

确。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。

7. 认证证书状态管理

认证证书的有效性通过公司对获证组织定期的监督获得保持。获证组织对于认证证书和认证标志的使用应遵守公司相关文件规定。公司按照《认证资格及证后管理程序》对不满足要求的认证证书实施暂停、撤销、变更等相应处置，同时按规定程序和要求报国家认监委。

7.1. 证书暂停

7.1.1. 当获证组织出现需要暂停证书的任何一种情形时，公司应在调查核实后的5个工作日内暂停其认证证书。

7.1.2. 认证证书暂停期不得超过6个月。但属于“资质等过期失效，重新提交的申请已被受理但尚未换证”的暂停期可至相关单位作出许可决定之日。

7.1.3. 公司应以适当方式公开暂停认证证书的信息，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。

7.1.4. 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，公司应恢复其认证资格，并保留相应证据。

7.2. 撤销证书

7.2.1. 当获证组织出现需要撤销证书的任何一种情形时，公司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。

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

7.3. 注销证书

获证组织主动申请不再保持认证资格时，公司应注销其认证资格，并保留相应证据。

更改记录：
