BSC-03-W-02-ISMS-2025

版号： B/0

信息安全管理体系认证规则

编制：聂咪咪 2025.08.06

审核：张 敬 2025.08.06

批准：孙竹君 2025.08.27

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

发布/实施日期：2025 年 8 月 27 日

目　录

1 适用范围

1.1 本规则用于规范依据 ISO 27001：2022《信息安全技术　信息安全管理体系　要求》标准开展的信息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，对信息安全管理体系认证实施过程作出具体规定，明确公司对认证过程的管理责任，保证信息安全管理体系认证活动的规范有效。

1.3 本规则是公司在信息安全管理体系认证活动中的基本要求，公司在该项认证活动中应当遵守本规则。除本文件规定的信息安全管理体系特定要求外，应遵循公司基本管理要求和各项管理制度。

2 认证依据

ISO 27001：2022《信息安全技术　信息安全管理体系　要求》

3 认证程序

3.1 受理认证申请

3.1.1 申请组织应满足以下条件：

(1) 取得国家市场监督管理部门注册登记的法人资格（或其组成部分），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（适用时）；

(3) 已按照ISO 27001 及相应行业认证要求建立了 ISMS 且体系正常运行三个月以上；且至少已实施一次完整内审和管理评审；

(4) 遵守有关主管部门对信息安全管理的强制性要求，或相关要求（适用时）；

(5) 两年内未发生信息安全事故或违反相关法规的情况（经审批可放宽至一年内）；

(6) 承诺遵守工信部联协[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（例如，工信部 2011 年第 21 号公告《工业和信息化部加强政府部门信息技术外包服务安全管理》）。

3.1.2 公司应当要求申请组织至少提交以下资料：

(1) 认证申请书，申请书应包括申请认证的生产、经营或服务活动范围及活动情况的说明；

(2) 法律地位的证明性文件：营业执照；法定许可文件、备案证明扫描件（适用时），如资质证书、许可证等；对管理体系覆盖多个法律实体时，应提供每个场所的法律地位证明性文件；

(3) 信息安全管理体系文件，包括 1）体系范围，2）方针，3）目标，4）信息安全风险评估准则及报告，5）信息安全风险处置计划，6）残余风险评估报告（适用时），7）适用的信息安全法律法规要求清单；8）网络拓扑结构图（适用时），9）组织机构图或职责说明，10）覆盖申请范围的1个或多个适用性声明（SOA）。

注：以上文件若包含在手册、程序文件中可不单独提供。

(4) 工信部安全审查备案（适用时）；

(5) 说明适用的关于认证机构的资质、信息安全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，以便判断公司是否具备对该客户实施认证活动的资格或条件（适用时）。

(6) 其他需要的文件。

3.1.3 公司应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。

3.1.4 对符合上述要求的，公司可决定受理认证申请；对不符合上述要求的，公司应通知申请组织补充和完善，或者不受理认证申请。

3.1.5 签订认证合同

3.1.5.1 公司根据评审结论与认证申请方签署《认证合同书》，信息安全管理体系相应内容应完整、清晰、准确无误。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。

3.1.5.2 认证合同应就控制审核和认证活动引发的客户信息安全风险做出规定，包括明确认证机构和客户及其有关人员的责任和义务。

3.2 审核策划

3.2.1 审核时间

3.2.1.1 为确保认证审核的完整有效，公司应根据申请组织信息安全管理体系覆盖的活动范围、特性、技术复杂程度、信息安全风险程度、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，可以减少审核时间，但减少的时间不得超过所规定的审核时间的 30%。审核时间的计算方法按照 CC170《信息安全管理体系审核和认证机构要求》相关要求执行。

3.2.1.2 整个审核时间中，现场审核时间不应少于总审核时间的 70%。

3.2.2 多场所抽样

（1）当客户拥有满足以下 a）至 c）的多个场所时，认证机构可以考虑使用基于抽样的方法进行多场所认证审核：

a）所有的场所在同一个 ISMS 下运行且该 ISMS 实行集中统一的管理、审核和管理评审；

b）所有的场所都包含在客户的 ISMS 内部审核方案中；

c）所有的场所都包含在客户的 ISMS 管理评审方案中。

（2）在使用基于抽样的方法时应确保：

a）在初次的合同评审时，最大程度地识别场所之间的差异，以便确定适当的抽样水平；

b）结合以下因素，认证机构抽取具有代表性的场所：

1）总部（适宜时）及各场所的内部审核结果；

2）管理评审的结果；

3）场所规模的差异；

4）场所业务范围的差异；

5）不同场所信息系统的复杂程度；

6) 工作实践的差异；

7) 所开展活动的差异；

8) 控制的设计与运行的差异；

9) 与关键信息系统或处理敏感信息的信息系统之间的潜在交互；

10）任何不同的法律要求；

11）地域因素和文化因素；

12）场所的风险状况；

13）特定场所发生的信息安全事件。

c）从客户 ISMS 范围内的所有场所中选择具有代表性的样本，该选择应基于一个可体现上述 b）中所列因素的判定，同时也考虑随机因素；

d）在授予认证之前，应审核了 ISMS 中每个具有重大风险的场所；

e）根据上述要求设计审核方案，且审核方案要在三年内覆盖 ISMS 认证范围内的代表性样本；

f）在单个场所发现不符合时，纠正措施程序的实施适用于证书所覆盖的所有场所。

审核应关注客户为确保单一的 ISMS 适用于所有场所并在运行层面实施统一管理所进行的活动。

审核应关注上述所有事项。

3.2.3 审核组

3.2.3.1 公司应当根据信息安全管理体系覆盖的活动的专业技术领域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。审核组中的审核员承担审核任务和责任。

3.2.3.2 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。

3.2.3.3 审核组可以有实习审核员，其要在审核员的指导下参与审核，不计入审核时间，不单独出具记录等审核文件，其在审核过程中的活动由审核组中的审核员承担责任。

3.2.4 审核计划

3.2.4.1 公司应为每次审核制定书面的审核计划。审核计划至少包括以下内容：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。

3.2.4.2 为使现场审核活动能够观察到产品生产或服务相关的信息安全管理情况，现场审核应安排在认证范围覆盖的产品生产或服务活动正常运行时进行。

3.2.4.3 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。

3.3 实施审核

3.3.1 文件审核

组长或组织相关审核员对受审核方的信息安全管理体系文件及必要的其它文件进行符合性评审，以确定审核的可行性，并确信能够实现审核目标。对评审中发现问题和评审结论应形成《文件评审报告》并提出明确的整改要求和时限。

3.3.2 第一阶段审核

3.3.2.1 审核组对申请组织的信息安全管理体系的第一阶段审核通常应在现场进行。第一阶段审核的目的是了解受审核方的基本信息、审核信息安全管理体系文件与审核准则的符合性、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，为第二阶段审核提供关注点，确定二阶段审核的可行性。

3.3.2.2 第一阶段审核应至少覆盖以下内容：

a）审核受审核方形成文件的信息安全管理体系信息的真实、准确、完整、有效性；

b）获取有关 ISMS 设计的文件，包括 ISO 27001 所要求的文件。

至少应包括：

——ISMS 和其所覆盖活动的一般信息；

—— ISO 27001 要求的 ISMS 文件的副本，以及需要时，其他相关文件。

c）应在客户的组织设置、风险评估与风险处置（包括所确定的控制）、信息安全方针和信息安全目标、适用性声明的背景下充分了解 ISMS 设计，特别是应充分了解客户的审核准备情况。

d）确认受审核方的 ISMS 范围和边界的界定是否清晰和充分。

e）通过现场观察，了解组织的基本概况，包括组织机构及职能，信息安全服务的流程和特点、活动的现场分布情况，提供过程中对资产的保密性、完整性及可用性要求，重要资产清单中所列资产的物理位置。应关注在服务和活动过程中和 ISMS 直接相关的重要场所：

- 信息安全管理体系推进部门；
- 核心信息处理设施的放置场所，如核心机房等；
- IT 部门，如信息系统的设计、开发及维护部门；
- 与重要信息资产有关的现场。

f）审查第二阶段审核所需资源的配置情况，并与申请组织商定第二阶段审核的细节；

g）评价组织对外包方的识别管理情况；

h）以上所了解的信息应用于策划第二阶段。并使客户知晓在二阶段审核中可以要求对更进一步的或其他类型的信息、文件、记录进行详细检查。

3.3.2.3 审核组应将第一阶段审核情况形成书面文件告知申请组织。对在第二阶段审核中可能被判定为不符合项的重要关键点，要及时提醒申请组织特别关注。

3.3.3 第二阶段审核

第二阶段审核应当在申请组织现场进行。重点是审核信息安全管理体系符合 ISO 27001 标准要求和有效运行情况，应至少覆盖以下内容：

a） 最高管理层对信息安全目标的领导和承诺；

b） 信息安全风险评估，包括确保在重复实施风险评估时能产生一致的、有效的和可比较的结果；

c） 根据信息安全风险评估和风险处置过程来确定控制；

d） 信息安全绩效和 ISMS 有效性，包括根据信息安全目标对其实施评价；

e） 所确定的控制、适用性声明、信息安全风险评估结果、风险处置过程与信息安全方针和信息安全目标之间的对应关系；

f） 控制的实现（见ISO27006标准附录 E－审核控制的示例）：审核应考虑外部环境、内部环境、相关风险以及组织对信息安全过程和控制的监视、测量与分析过程，并确定待实现的控制是否已经实现且在整体上是有效的；

g）方案、过程、规程、记录、内部审核和对 ISMS 有效性的评审，且这些都能追溯到最高管理层的决定、信息安全方针和信息安全目标。

3.3.4 发生以下情况时，审核组应向公司报告，经公司同意后终止审核。

（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。

3.4 审核报告

3.4.1 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。审核报告应准确、简明和清晰地描述审核活动的主要内容，除应满足其他管理体系通用的要求外，还包括以下内容：

a） ISMS 管理体系范围、过程、场所的必要信息；

b） 所采用的主要审核路线和所使用的审核方法；

c） 客户信息安全风险分析的审核情况说明；

d） 客户在实施 ISO/IEC 27001:2022 6.1.3 c）所要求的比较时，所使用的任何信息安全控制集；

e） 所引用的适用性声明版本，以及适用时，与客户以往认证审核结果的任何有用的比较；

注：完成的问卷、检查清单、评论意见、日志或审核员笔记可以构成审核报告的组成部分。如果使用了这些方法，这些文件应作为支持认证决定的证据提供给公司。有关审核中所评价的样本的信息，应包含在审核报告或其他认证资料中。

f） 如果使用了远程审核方法，报告应说明远程审核方法在审核中的使用程度及其实现审核目标的有效性；

g） 当组织的活动不是在明确的物理位置实施的，而是其所有活动都是远程实施的时，审核报告应说明组织所有活动都是远程实施的；

h） 报告应考虑客户所采用的内部组织和规程的充分性，以便对其 ISMS 建立信心。受审核方的 ISMS 管理体系符合标准的情况，如方针、目标指标和管理要

求的实施完成情况，重要信息安全风险是否都得到控制，各种程序文件和作业指导书的执行情况等；

i）受审核方 ISMS 管理体系实施的适宜性和有效性，包括改进机会等；应概述关于 ISMS 要求和信息安全控制的实现与有效性的最重要评论意见（正面的和负面的）；

j）审核发现的不符合项概述，以及实施完成纠正措施的要求； 不符合项纠正措施有效性验证情况；

k）是否偏离审核计划的情况。

3.5 不符合项的纠正和纠正措施及其结果的验证

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，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、保持认证或再认证。

3.6 认证决定

3.6.1 认证评定人员根据对审核过程中收集的信息以及审核过程之外获取的任何可作为认证决定依据的信息（如来自行政监管部门、顾客、行业协会的信息等）进行复核，审核过程中对认证范围、关键过程的实施等方面重点关注，技术委员会主任对认证决定的结果进行批准。

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

3.6.3 为确保公正性，所有参与认证决定的人员不能是实施审核的人员。对经审定不合格的申请组织，公司应做出不予以认证注册的决定，并将不能注册的原因书面通知申请组织。

4 监督审核程序

4.1 公司应对持有其颁发的信息安全管理体系认证证书的获证组织进行有效跟踪，监督获证组织持续运行信息安全管理体系并符合认证要求。

4.2 作为最低要求，初次认证后的第一次监督审核应在认证证书签发日起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。

4.3 监督审核的时间，应不少于初审审核时间人日数的 1/3。

4.4 监督审核应在获证组织现场进行，但不一定是对整个体系的审核，除应满足管理体系认证通用要求外，还应包括下述方面的审核内容：

a）ISMS在实现客户信息安全方针的目标方面的有效性；

b）相关信息安全法律法规合规性的定期评价和审查规程的运行情况；

c）所确定的控制的变更，及其引起的适用性声明变更；

d）审核方案中所述控制的实现和有效性。

5 再认证程序

5.1 认证证书期满前，若获证组织申请继续持有认证证书，公司应当实施再认证审核，并决定是否延续认证证书。

5.2 公司应按本文件要求组建审核组。结合历次监督审核情况，制定再认证审核计划交审核组实施。

5.3 在信息安全管理体系及获证组织的内部和外部环境无重大变更时，再认证审核可省略第一阶段审核，但审核时间应不少于初审审核人日数的 2/3。

5.4再认证审核还应关注以下内容：

a）对获证客户的业绩评价和文件再评审（需安排在现场审核前进行）；

b）审查获证客户针对保持管理体系有效性和改进管理体系提高整体绩效的承诺的证据；

c）再认证应考虑在最近一个认证周期内的绩效情况；

d）客户的管理体系在实现目标和预期结果方面的有效性。

6 认证证书和认证标志要求

6.1 认证证书应至少包含以下信息：

（1）获证组织名称、地址和统一社会信用代码（或组织机构代码）。该信息应与其法律地位证明文件的信息一致。

（2）信息安全管理体系覆盖的生产经营或服务的地址和业务范围。若认证的信息安全管理体系覆盖多场所，表述覆盖的相关场所的名称和地址信息。

（3）信息安全管理体系符合 ISO 27001 标准的表述。

（4）证书编号。

（5）有效期的起止年月日。

（6）相关的认可标识及认可注册号（适用时）。

（7）证书查询方式。公司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。

6.2 初次认证认证证书有效期最长为 3 年。获证组织必须定期接受监督审核并经审核合格此证书方继续有效的提示信息。

6.3认证申请组织通过认证并获得认证证书后，可以在认证范围内使用认证标志。但应当遵守以下规定：

（1）保证使用认证标志符合认证要求；

（2）在广告、服务项目介绍等宣传材料中正确地使用认证标志、不得利用认证标志误导消费者；

（3）接受国家认证认可监督委员会、各地质检行政部门和机构对认证标志使用情况的监督审查；

（4）当认证证书被暂停、注销或撤消认证时，应停止使用认证标志和发放带有认证标志的所有文件和宣传资料。

6.4 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，并已在公司网站公示。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

信息安全管理体系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。公司按照《认证证书和认证标志管理办法》对认证证书实施暂停、恢复、撤销、变更等相应处置，并在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。

7.1 暂停证书

7.1.1 获证组织出现以下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：

（1）信息安全管理体系持续或严重不满足认证要求，包括对信息安全管理体系运行有效性要求的。

（2）不承担、履行认证合同约定的责任和义务的。

（3）被有关执法监管部门责令停业整顿的。

（4）持有的与信息安全管理体系范围有关的行政许可证明、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。

（5）主动请求暂停的。

（6）其他应当暂停认证证书的。

7.1.2 认证证书暂停期不得超过 6 个月。

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。

7.2 恢复证书

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。

7.3 撤销证书

7.3.1 获证组织出现以下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：

（1）被注销或撤销法律地位证明文件的。

（2）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。

（3）有其他严重违反法律法规行为的。

（4）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（包括持有的与质量管理体系范围有关的行政许可证明、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）。

（5）没有运行信息安全管理体系或者已不具备运行条件的。

（6）其他应当撤销认证证书的。

7.3.2 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。

7.4 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：
